AFIATUL SYAHRIZAT BT MOHD HARIS

WEK 990421

SISTEM PENGANALISA RANGKAIAN (NAs)

SARJANA MUDA SAINS KOMPUTER

ABSTRAK

Sistem Penganalisa Rangkaian (NAs) merupakan tajuk untuk latihan ilmiah saya bagi memenuhi keperluan Ijazah Sarjana Muda Sains Komputer. Projek ini di bawah penyeliaan Cik Fazidah Othman, merupakan sebuah sistem pemantauan aktiviti rangkaian (LAN) "standalone" dan interaktif.

Sistem ini dibangunkan berlandaskan kehendak penggunanya yang lebih ditumpukan kepada pentadbir dan jurutera rangkaian sendiri. Sistem ini dapat membantu pentadbir rangkaian dalam memantau aktiviti semasa rangkaian. Ini membolehkan pentadbir rangkaian mendapatkan statistik aktiviti-aktiviti rangkaian yang berjalan yang merangkumi aktiviti internet dan keluar masuk data di dalam rangkaian.

Sistem ini dibangunkan menggunakan perisian Microsoft Visual Basic 6.0, Microsoft Access 2000, dan boleh dilarikan pada persekitaran sistem pengendalian Windows 98 atau lebih.

----------PENGHARGAAN----------

Alhamdulillah, bersyukur saya ke hadrat illahi kerana dengan izinnya, maka saya dapat menyempurnakan projek Latihan Ilmiah ini. Walaupun jangkamasa yang diperuntukkan untuk menyiapkan projek ini adalah terhad, disamping tugasan-tugasan matapelajaran lain, namun berkat sokongan dan dorongan yang telah diberikan oleh pelbagai pihak, maka projek ini dapat dijalankan dengan baik.

Dikesempatan ini, saya ingin mengucapkan jutaan terima kasih kepada ***Cik Fazidah Othman****, selaku penyelia projek ini, di atas tunjuk ajar dan bantuan yang telah diberikan dari peringkat awal lagi. Tidak lupa juga ucapan terima kasih ini ditujukan buat* ***Puan Miss Laiha Mat Kiah****, selaku moderator bagi latihan ilmiah I dan* ***En. Amirrudin Kamsin****, selaku moderator latihan ilmiah II.*

Sekalung penghargaan ditujukan kepada keluarga tersayang terutama buat ayahanda, ***Mohd Haris Bin Alias****, dan bonda,* ***Sharifah Azizah Abdullah****, di atas sokongan dan dorongan yang telah diberikan sepanjang pengajian saya di Fakulti Sains Komputer dan Teknologi Maklumat ini, serta bantuan dari segi kewangan sehingga membolehkan saya menyiapkan projek Latihan Ilmiah ini.*

Jutaan terima kasih juga buat rakan-rakan yang banyak membantu dalam menjayakan projek ini terutama kepada saudara Raja Khuzairi yang banyak membantu dan berkongsi pengetahuan dalam menyempurnakan projek ini. Dan tidak lupa juga ucapan terima kasih ditujukan kepada Saiful Naim, Nuha, Pissa, Mary, Along, Alen, Idot dan semua rakan-rakan di atas bantuan, galakan, dan sokongan yang diberikan.

Sekian, terima kasih.

Afiatul Syahrizat Binti Mohd Haris

Sarjana Muda Sains Komputer

Fakulti Sains Komputer Dan Teknologi Maklumat, Universiti Malaya.

ISI KANDUNGAN

SENARAI RAJAH

SENARAI JADUAL

BAB 1: PENGENALAN SISTEM

Ethernet dibina di dalam persekitaran kepentingan perkongsian, di mana semua mesin di dalam rangkaian tempatan membuat perkongsian di dalam wayar yang sama. Ini membayangkan bahawa semua mesin boleh atau dapat melihat semua trafik di dalam wayar yang sama. Oleh yang demikian, perkakasan Ethernet telah dibina bersama "penapis" yang mengabaikan trafik-trafik yang tidak dimiliki oleh sesuatu mesin itu. Ini dilakukan dengan mengabaikan semua kerangka (frame) yang tidak sama atau secocok dengan alamat MAC.

Maka, program "wiretap" memadamkan fungsi penapis ini, dan meletakkan perkakasan Ethernet tersebut di dalam mod campuran (promiscuous mode).

Sistem Penganalisa Rangkaian (NAs) ini, direkabentuk untuk dibangunkan di dalam persekitaran rangkaian. Ia dibangunkan, bagi membantu pentadbir rangkaian memantau keadaan trafik rangkaian. Dan ini dilakukan dengan mengubah suatu sambungan Ethernet, agar dapat menerima dan menangkap paket-paket pengguna rangkaian yang lain.

Dengan cara ini, maka pentadbir rangkaian dapat membuat analisa dengan melihat kepada statisitik protokol, port, atau alamat IP. Dan dengan ini, secara tidak langsung, membantu pentadbir rangkaian mengesan pencerobohan oleh penjenayah-penjenayah siber.

1.1 Definasi Projek

Pada masa sekarang, rangkaian komputer direkabentuk agar dapat menampung pelbagai permintaan pengguna. Permintaan yang dijalankan adalah seperti penghantaran fail, login jarak jauh, mel elektronik, dan "newsgroup", melibatkan pelbagai aktiviti rangkaian . Pemantauan ke atasnya perlu bagi membolehkan pentadbir rangkaian membuat analisa ke atas aktiviti-aktiviti yang berjalan.

Sistem Penganalisa Rangkaian merupakan sebuah sistem yang dibangunkan untuk tujuan menganalisa rangkaian. Sistem ini dapat merekodkan aktiviti-aktiviti rangkaian. Aktiviti-aktiviti rangkaian ini termasuk aktiviti-aktiviti internet dan keluar masuk data di dalam rangkaian yang direkodkan bertujuan untuk mendapatkan statistiknya.

Analisa rangkaian dijalankan dengan mengambilkira statistik aktiviti-aktiviti rangkaian yang telah direkodkan itu. Statistik-statistik ini direkodkan dengan menggunakan kaedah penapisan. Kaedah ini dijalankan ke atas 3 bahagian penting iaitu alamat IP, protokol, dan port. Ketiga-tiga bahagian ini ditapis dan dibahagikan kepada jenis-jenisnya tertentu.

Oleh itu, sistem ini merupakan sebuah sistem yang mampu dalam mengesan masalah-masalah yang berlaku di dalam rangkaian dan dijangkakan menjadi sebuah sistem perisian yang mampu bersaing dalam situasi rangkaian komputer dunia yang kini sedang melalui zaman perkembangan teknologi maklumat.

1.2 Pernyataan Masalah

Memandangkan pada hari ini, penggunaan rangkaian komputer semakin meningkat dan berkembang, maka penyalahgunaan rangkaian ini juga semakin meningkat. Bagi membendung dan memantau gejala ini, maka sistem penganalisa rangkaian ini dibangunkan bagi membantu pentadbir rangkaian memantau rangkaian bagi memastikan masalah penyalahgunaan rangkaian ini terkawal.

Permintaan untuk analisis rangkaian bergantung kepada suatu set primitif yang sesuai untuk menangkap paket. Hampir kesemua sistem Unix memiliki modul kernel yang menyokong sekurang-kurangnya penangkapan paket, tetapi keupayaan bagi Windows adalah kurang memberangsangkan. Sistem Penganalisa Rangkaian ini dibangunkan bagi memenuhi kehendak pengguna Windows. Sistem ini menyokong semua sistem pengendalian bagi windows 98 dan lebih.

1.3 Objektif Sistem

Sistem Penganalisa Rangkaian ini dibangunkan adalah bertujuan untuk membantu kerja-kerja pentadbir rangkaian dan jurutera rangkaian. Diantara objektif-objektif sistem ini dibangunkan adalah:

1. Pemantauan dari semasa ke semasa ke atas rangkaian LAN dapat dilakukan dengan lebih mudah.

   Penggunaan Sistem Penganalisa Rangkaian ini, dapat membantu pentadbir rangkaian dalam menjalankan tugas-tugasnya terutamanya dalam memantau aktiviti-aktiviti rangkaian oleh penggunanya. Apabila sesuatu paket data dihantar di antara satu komputer ke komputer lain, maka dengan menggunakan kaedah "listen", sesuatu paket data yang dihantar ditangkap (capture) dan salinan ke atas data-data tersebut diambil. Dengan cara itu, pentadbir rangkaian dapat mengetahui aktiviti-aktiviti yang dilakukan seterusnya membuat analisa ke atasnya.

2. Penyalahgunaan di dalam rangkaian dapat di kesan dengan mudah.

   Dengan pemantauan yang dijalankan oleh pentadbir rangkaian, maka mereka dapat mengesan kesalahan-kesalahan yang dilakukan oleh pengguna di dalam rangkaian. Kesalahan-kesalahan seperti suntikan virus dan "hacking" dapat dikesan. Maka, jurutera rangkaian dapat mengambil langkah sewajarnya dengan merekabentuk sebuah sistem rangkaian yang selamat dan terkawal bagi mengawal perkara-perkara ini.

3. Analisa ke atas rekod pemantauan rangkaian dapat dilakukan untuk mengenalpasti punca/masalah yang berlaku kc atas rangkaian melalui statistik dan graf.

4. Membantu meningkatkan kepekaan terhadap situasi rangkaian dari semasa ke semasa untuk meningkatkan tahap keselamatan rangkaian sedia ada.

1.4 Skop Projek

1.4.1 Persekitaran

Sistem Penganalisa Rangkaian ini dibangunkan adalah untuk memantau kegiatan-kegiatan pengguna rangkaian. Sistem ini direka untuk kegunaan di dalam satu persekitaran rangkaian LAN (Local Area Network). LAN biasanya dimiliki oleh sesebuah organisasi dan peranti-peranti perkakasannya dihubungkan di dalam sesebuah pejabat, bangunan, atau kampus. LAN direkabentuk untuk membolehkan sumber-sumber seperti perkakasan, perisian atau data dikongsi diantara komputer peribadi dan stesen-stesen kerja yang lain.

1.4.2 Pengguna Sasaran

Sistem ini dibangunkan untuk kegunaan Pentadbir Rangkaian dan Jurutera Rangkaian. Pentadbir Rangkaian menggunakan sistem ini bagi membantu mereka menjalankan tugas-tugas pentadbiran rangkaian. Tugas-tugas pentadbiran rangkaian ini termasuklah menstabilkan trafik di dalam laluan rangkaian, memastikan rangkaian sentiasa dapat digunakan oleh penggunanya, memantau aktiviti-aktiviti pengguna di dalam rangkaian, memastikan persekitaran rangkaian selamat daripada ancaman virus, dan mengambil langkah-langkah keselamatan bagi mengawal penyebaran virus yang masuk ke dalam rangkaian.

Dengan menggunakan sistem ini, pentadbir rangkaian dapat membuat analisa ke atas penggunaan trafik rangkaian dan boleh mengesan penyalahgunaan yang berlaku di dalam sesuatu rangkaian. Bagi jurutera rangkaian, untuk membangunkan perkakasan yang betul dan baik merupakan satu cabaran. Rekabentuk sambungan di antara komputer peribadi, stesen-stesen kerja dan peranti digital lain memerlukan kefahaman tentang keperluan pengguna. Begitu juga bagi menangani isu-isu penyalahgunaan rangkaian yang dilakukan oleh pengguna rangkaian. Sistem Penganalisa Rangkaian ini, berguna untuk membantu seorang jurutera rangkaian mengenalpasti kesalahan-kesalahan yang kerap kali terjadi di dalam rangkaian tersebut. Seterusnya, merekabentuk suatu sistem rangkaian yang dapat mengawal penyalahgunaan yang berlaku.

1.4.3 Had Masa Perlaksanaan

Kebiasaannya, pengguna-pengguna rangkaian tidak menghadkan penggunaan rangkaian. Maka, penggunaan ke atas rangkaian boleh dilakukan pada bila-bila masa (24 jam sehari). Oleh yang demikian, Sistem Penganalisa Rangkaian ini perlu dilarikan dan dijalankan sepanjang masa. Dengan kata lain, tiada had masa yang diperuntukkan untuk perlaksanaan sistem ini iaitu, selama mana sesuatu rangkaian itu berfungsi. Bagaimanapun, pentadbir rangkaian perlu menentukan tempoh sistem ini dilarikan, sebelum analisa ke atas aktiviti-aktiviti rangkaian dibuat. Ini juga bergantung kepada jenis organisasi yang mengimplimentasikan LAN seperti pejabat, kolej, institusi-institusi pengajian tinggi, organisasi swasta atau kerajaan dan lain-lain. Contohnya, bagi sebuah pejabat, seorang pentadbir rangkaian boleh membuat analisa ke atas rangkaian selepas 1 minggu sistem ini dilarikan, dan boleh dibuat pada luar waktu pejabat, dimana penggunaan rangkaian adalah minimum.

1.5 Keperluan Sistem

Keperluan sistem dibahagikan kepada 2 bahagian iaitu perkakasan dan perisian. Berikut merupakan speifikasi perkakasan dan perisian yang diperlukan bagi membolehkan sistem berfungsi dengan baik.

1.5.1 Spesifikasi Perkakasan

- Komputer peribadi IBM dan bersesuaian
- Pemproses mikro, sekurang-kurangnya 233Mhz
- RAM, sekurang-kurangnya 32Mb
- Ruangan storan, sekurang-kurangnya 10Mb cakera keras.
- Monitor, sekurang-kurangnya, 800x600 pixel
- Peranti input, papan kekunci dan tetikus

1.5.2 Spesifikasi Perisian

- Microsoft Visual C++ 6.0
- Microsoft Access 2000
- WinPcap
- Sistem Pengendalian (Windows 98 dan ke atas)

1.6 Hasil Jangkaan

Sistem Penganalisa Rangkaian ini dijangkakan dapat memenuhi kehendak sistem rangkaian pada masa ini sejajar dengan pembangunan teknologi maklumat pada hari ini.

Sistem ini dijangkakan dapat membantu pentadbir rangkaian dalam menjalankan tugas-tugasnya terutamanya di dalam bahagian pemantauan rangkaian. Sistem ini diharap dapat membendung masalah dengan mengesan punca-punca masalah seperti mengesan ketidakstabilan laluan trafik yang berlaku di dalam rangkaian, memantau data-data semasa yang keluar masuk dari rangkaian dan memastikan keperluan pengguna rangkaian dipenuhi selagi tidak melanggar peraturan-peraturan yang ditetapkan.

Selain itu, sistem ini juga diharapkan dapat memberikan statistik tepat tentang aktiviti-aktiviti rangkaian seperti keluar masuk data dan aktiviti-aktiviti internet, dengan memberikan nilai yang tepat atas setiap satunya. Ini kerana pada hari ini kebanyakan statistik yang dibuat adalah mengambil nilai secara rawak dan kebanyakannya tidak tepat dan ini tidak menjamin keukuhan sesuatu rangkaian komputer itu.

Sistem ini juga diharapkan dapat membantu dalam mengesan penyalahgunaan di dalam rangkaian komputer, yang kini menjadi salah satu cabaran besar dalam mengharungi kemajuan dalam dunia IT pada hari ini.

1.7 Penjadualan Projek

Fasa-fasa peringkat bagi perlaksanaan projek pembangunan Sistem Penganalisa Rangkaian (NAs) ini ditunjukkan seperti di dalam carta gantt di bawah.

Bil	Fasa-fasa	2002							2003	
		Jun	Jul	Ogos	Sept	Okt	Nov	Dis	Jan	Feb
1	Kajian awal dan analisis sistem									
2	Merekabentuk sistem									
3	Perlaksanaan sistem									
4	Pengujian sistem									
5	Penyelenggaraan sistem									

Jadual 1.1 : Carta Gantt bagi penjadualan projek untuk NaS

BAB 2 : KAJIAN LITERASI

Bab ini menerangkan tentang hasil kajian yang lebih lanjut yang berkaitan dengan projek yang dijalankan dan isu-isu yang berkaitan. Isu-isu yang dibincangkan di sini adalah meliputi definasi bagi beberapa istilah yang berkaitan, dan pendekatan-pendekatan yang diambil sebagai perbandingan dan kajian ke atas NAs.

2.1 LAN (Local Area Network)

LAN atau Rangkaian Kawasan Setempat, merupakan salah satu daripada 3 kategori rangkaian primer (LAN,MAN,WAN). LAN biasanya adalah milik persendirian bagi sesebuah organisasi yang merangkaikan peranti-peranti di dalam organisasi tersebut agar mereka dapat berkomunikasi antara satu sama lain.

LAN membawa mesej pada kelajuan tinggi di antara komputer-komputer, yang dihubungkan melalui medium komunikasi tunggal, seperti kabel UTP, kabel coaxial atau kabel fiber optik. Suatu **segmen** ialah seksyen dimana yang berkhidmat untuk suatu jabatan atau suatu tingkat yang mana boleh mempunyai banyak komputer berhubung antara satu sama lain. Tiada laluan mesej diperlukan di dalam persekitaran suatu segmen, selagi medium tersebut menyediakan sambungan terus antara semua komputer yang berhubung melaluinya. Jumlah "bandwith" sistem adalah dikongsi diantara komputer-komputer yang bersambung pada segmen tersebut. Sistem rangkaian yang lebih besar seperti mana yang bertindak di dalam sebuah bangunan atau kampus, adalah dihubungkan melalui banyak segmen yang di hubungkan melalui switch atau hub. Di

dalam LAN, jumlah "bandwith sistem adalah tinggi dan "latency" adalah rendah kecuali apabila trafik mesej tinggi.

Beberapa teknologi rangkaian LAN ini telah dibina pada sekitar tahun 1970an (Ethernet, token rings and slotted rings). Setiap satunya membekalkan prestasi yang baik dan efektif dalam penyelesaian masalah rangkaian. Tetapi Ethernet telah muncul sebagai teknologi dominan dalam pengkabelan LAN. Ia telah mula diperkenalkan pada awal 1970an dengan "bandwith" 10Mbps dan meningkat kepada 100Mbps dan 1000Mbps (1 gigabit persecond) baru-baru ini.

LAN dibezakan daripada kategori rangkaian yang lain melalui media transmisinya dan jenis topologinya. Secara amnya, LAN menggunakan hanya satu jenis media transmisi. Dan topologi yang biasanya digunakan dalam rangkaian ini adalah bus, ring, dan star.

2.2 Pemindahan Paket

Di dalam kebanyakan aplikasi rangkaian komputer, keperluannya adalah pemindahan unit logikal bagi maklumat atau mesej. Maklumat atau mesej ini terdiri daripada urutan data-data yang mempunyai ukuran rawak. Tetapi sebelum mesej-mesej ini dihantar, ia dibahagikan kepada paket-paket. Paket yang paling ringkas ialah urutan bagi data binari (jujukan bagi bits atau bait) untuk panjang yang terbatas, bersama-sama maklumat yang perlu seperti alamat untuk mengenalpasti sumber dan destinasi komputer. Paket-paket ini digunakan untuk:

- Membolehkan setiap komputer di dalam rangkaian memperuntukkan storan penimbal yang memadai bagi memegang paket terbesar yang berkemungkinan datang.
- Mengelakkan tundaan masa yang tidak sepatutnya, yang selalu berlaku ketika menunggu rangkaian komunikasi menjadi sedia ada untuk digunakan dalam menunggu sesuatu mesej lain dilaksanakan.

2.3 Heksadesimal

Semua data di dalam komputer dipersembahkan dalam bentuk angka (nombor). Heksadesimal merupakan sistem penomboran yang lebih baik bagi memaparkan data berbanding nombor desimal. Heksadesimal merupakan satu konsep Sains Komputer.

Perkataan "decimal" mempunyai awalan "dec" yang bererti "10". Ini bermakna terdapat 10 digit di dalam system penomboran ini iaitu:

0 1 2 3 4 5 6 7 8 9

Perkataan "hexadecimal" pula mempunyai awalan "hex" yang bererti "6" dan "dec" yang bererti "10", kedua-duanya ditambah, dan akan mendapat hasil 16. Ini bermakna terdapat 16 di dalam system penomboran ini.

0 1 2 3 4 5 6 7 8 9 A B C D E F

Semua data disimpan di dalam komputer sebagai "bits" (binary-digits) yang bermembawa erti 2 digit : 0 1, tetapi semua bit tersebut diletakkan dibawah satu kumpulan 8 bit dan dikenali sebagai "bytes" atau "octects", yang mana di dalam teori mempunyai 256 digit. Bit adalah terlalu kecil untuk memaparkan data, kerana apa yang boleh dilihat adalah aliran digit yang sukar dibaca seperti berikut:

00101010101000010101010110101101101011110110

Heksadesimal membenarkan juruteknik untuk membayangkan data binari tersebut. Mereka mempunyai jadual ingatan seperti berikut:

0000 = 0 0001 = 1 0010 = 2 0011 = 3

0100 = 4 0101 = 5 0110 = 6 0111 = 7

1000 = 8 1001 = 9 1010 = A 1011 = B

1100 = C 1101 = D 1110 = E 1111= F

Heksadesimal biasanya di dahului dengan simbol-simbol yang unik. Sebagai contoh, bagi nombor 12, adakah ia merupakan 12 bagi penomboran desimal atau 18 bagi penomboran heksadesimal? Jika ianya adalah heksadesimal, ia akan ditulis sebagai "0x12", "0x12", atau "$12".

2.4 Kod ASCII

Komputer mempersembahkan segalanya dalam bentuk nombor. Ini bermakna setiap teks yang terpapar di dalam komputer juga dipersembahkan sebagai nombor di dalam persekitaran komputer. Di dalam ASCII, huruf 'A' adalah mewakili nombor 65, atau di dalam heksadesimal, 0x41. Huruf 'B' pula, mewakili nombor 66, atau di dalam heksadesimalnya 0x42. Proses ini berterusan untuk semua aksara, nombor, tanda bacaan, dan sebagainya.

Jika dilihat pada papan kekunci biasa, terdapat 32 tanda bacaan, 10 nombor desimal, dan 26 huruf yang boleh diubah paparannya sama ada huruf besar atau huruf kecil. Maka jumlah keseluruhannya adalah 94 aksara yang berbeza. Di dalam penduaan, memerlukan 7 bit untuk memaparkan kombinasi nombor tersebut. Ini dipetakan kepada 8 bit bait yang digunakan di dalam komputer. Di dalam heksadesimal, ruang ASCII mempunyai banyak lewahan. Satu bait mempunyai 256 kombinasi, tetapi hanya 94 sahaja daripadanya yang boleh dipaparkan. Aksara lain yang tidak termasuk di dalam 94 ini, ditunjukkan sebagai lewahan.

2.5 Lapisan OSI (Open Systems Interconnection)

Model OSI merupakan lapisan rangka kerja untuk rekabentuk sistem rangkaian yang membenarkan komunikasi antara semua jenis sistem komputer. Ia merupakan piawaian bagi ISO (International Standards Organization) yang menyentuh aspek komunikasi rangkaian. OSI terdiri daripada 7 lapisan yang berasingan tetapi berhubung kait antara satu sama lain. Lapisan–lapisan tersebut adalah fizikal, data link, rangkaian, pengangkutan, sesi, persembahan, dan aplikasi.

2.5.1 Lapisan Fizikal

Lapisan fizikal membawa bit data ke dalam wayar atau medium perantaraan. Wayar yang berbeza memerlukan cara yang berbeza untuk mengekod bit. Ethernet, menukarkan bit kepada suatu siri lapisan voltan yang tinggi / rendah.

2.5.2 Lapisan Data Link

Konsep yang penting dalam mengingati lapisan data link ini ialah "next hop". Ia bertujuan untuk menyambungkan 2 mesin bersama. Di dalam wayar Ethernet, mesin mengikat bersama paket IP dan maklumat Ethernet, dan menghantar ia kepada router pertama. Router itu kemudiannya akan menanggalkan pengepala (header) Ethernet . Router tersebut kemudiannya menentukan arah untuk menghantar paket, dan

menggabungkan ia bersama maklumat kerangka Data Link untuk menyeberangi wayar dan pergi ke router berikutnya.

Suatu mesin boleh memiliki alamat Ethernet "MAC" dan alamat IP. Ethernet merupakan lapisan Data Link, dan alamat MAC hanya wujud secara setempat, dan digunakan oleh router setempat dalam mengetahui cara menghantar trafik yang datang.

2.5.3 Lapisan Rangkaian

Lapisan rangkaian ini bertanggungjawab dalam penghantaran paket sumber ke destinasi yang menyeberangi pelbagai rangkaian. Lapisan data link mengawasi penghantaran paket diantara 2 sistem di dalam rangkaian yang sama, manakala lapisan rangkaian ini pula memastikan setiap paket adalah asli sehingga ia sampai ke destinasinya.

2.5.4 Lapisan Pengangkutan

Lapisan pengangkutan ini bertanggungjawab dalam penghantaran hujung ke hujung seluruh mesej. Lapisan rangkaian mengawasi penghantaran hujung ke hujung bagi paket individu, ia tidak dapat mengenalpasti apa-apa perhubungan diantara paket-paket tersebut. Lapisan pengangkutan ini memastikan keseluruhan mesej tiba dengan sempurna dan mengikut apa yang diingini, juga ia mengawasi kawalan ke atas kesilapan dan kawalan aliran pada lapisan sumber ke destinasi.

2.5.5 Lapisan Sesi

Lapisan sesi merupakan jurukawal dialog rangkaian. Ia bertindak mengukuhkan, mengekalkan, dan menyegerakkan interaksi diantara sistem komunikasi. Di antara tanggungjawab lapisan ini adalah seperti berikut:

- **Kawalan Dialog** - Lapisan sesi ini membenarkan 2 sistem untuk berdialog. Dan komunikasi dibenarkan sama ada dalam half-duplex atau full-duplex.
- **Kesegerakan** – Lapisan ini juga membenarkan suatu proses menambah titik kesegerakan di dalam suatu aliran data.

2.5.6 Lapisan Persembahan

Lapisan ini mementingkan sintak dan semantik bagi pertukaran maklumat di antara 2 sistem. Di antara tanggungjawab lapisan ini adalah:

- **Terjemahan** – Suatu proses (program yang sedang berjalan) di dalam 2 sistem biasanya bertukar maklumat dalam bentuk aksara, string, nombor dan bermacam lagi. Maklumat ini perlu ditukar dalam bentuk aliran bit sebelum ia dihantar. Oleh kerana komputer yang berlainan menggunakan pengekodan yang berlainan, lapisan persembahan ini bertanggungjawab dalam membuat terjemahan ke atas kaedah pengekodan 2 sistem yang berbeza ini.

- **Enkripsi** – Bagi tujuan membawa maklumat yang sulit, suatu system perlu memastikan keselamatan yang terjamin. Maka dengan ini kaedah enkripsi ini diperlukan.
- **Pemampatan** – Pemampatan data dapat mengurangkan bilangan bit yang perlu dipindahkan dan ia menjadi sangat penting di dalam pemindahan / penghantaran multimedia seperti teks, audio, dan video.

2.5.7 Lapisan Aplikasi

Lapisan ini bukan bermakna aplikasi yang dijalankan, tetapi protokol yang menjalankan kerja-kerja untuk aplikasi. Contohnya HTTP untuk browser web, SMTP / POP / IMAP untuk emel.

2.6 Bahagian-bahagian untuk penapisan

Di dalam mengimplementasikan NaS ini, terdapat tiga bahagian penting yang akan diambilkira untuk ditapis bagi mendapatkan maklumat-maklumat yang diperlukan bagi memenuhi kehendak sistem yang akan dibangunkan. Bahagian-bahagian tersebut ialah:

- Protocol
- Alamat IP
- Port

2.6.1 Protokol

Protokol digunakan untuk mewakili suatu set peraturan dan format yang perlu digunakan untuk komunikasi diantara proses-proses di dalam menjalankan tugas-tugas yang telah diberikan. Terdapat 2 bahagian penting dalam memberi definasi ke atas protokol:

- Suatu spesifikasi bagi urutan mesej-mesej yang perlu ditukar ganti.
- Suatu spesifikasi bagi format data di dalam mesej.

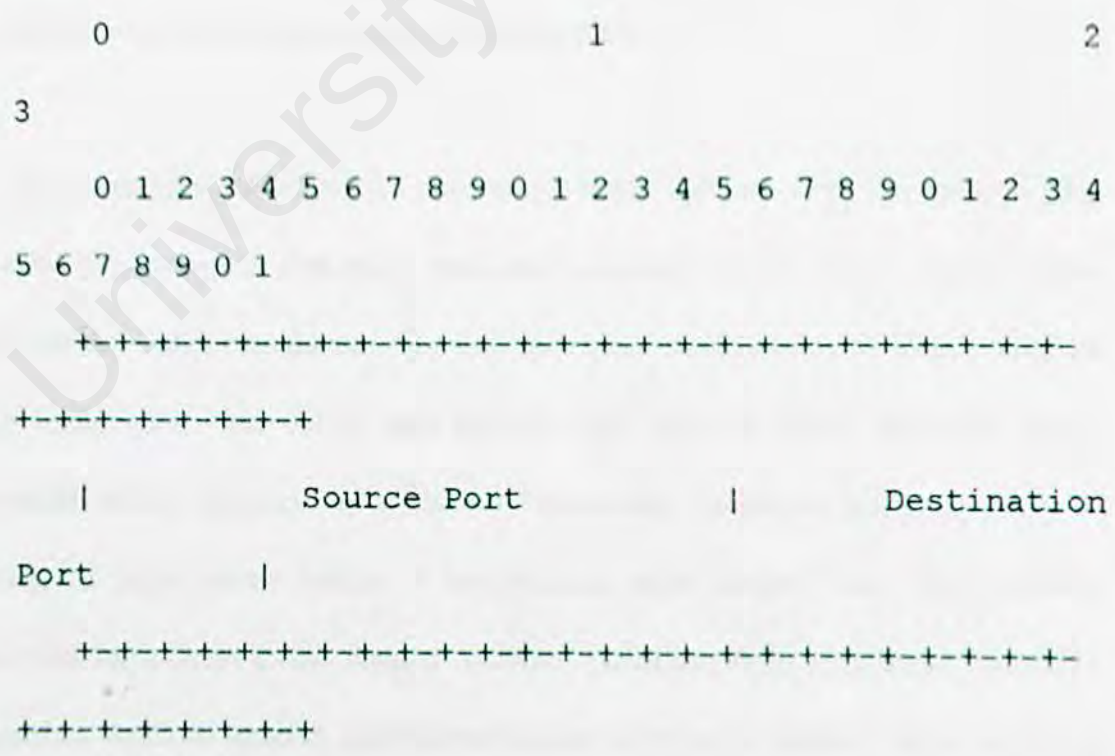
Suatu protokol dibina oleh modul perisian yang bertempat di dalam komputer penghantar dan penerima. Sebagai contoh, *transport protocol* menghantar mesej yang pelbagai ukuran daripada proses penghantar kepada proses penerima. Suatu proses yang perlu menghantar mesej kepada suatu proses lain memerlukan modul *transport protocol* yang akan memberikan mesej tersebut di dalam format yang telah ditentukan. Perisian penghantar kemudiannya membahagikan mesej tersebut kepada paket-paket di dalam dengan format dan saiz tertentu yang membolehkan ia dihantar kepada destinasinya melalui *network protocol*. Modul *transport protocol* yang sama di dalam komputer penerima, menerima paket melalui modul *network-level protocol* dan memberikan pertukaran terbalik untuk menghasilkan semula meej sebelum memberikan ia kepada proses penerima.

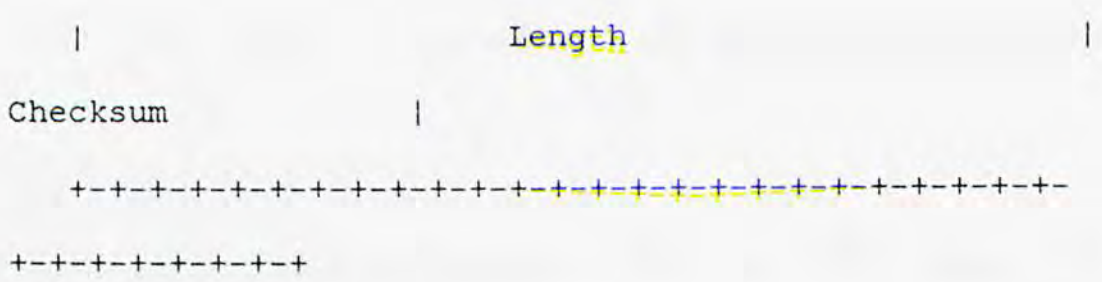
2.6.1.1 UDP (User Datagram Protocol)

UDP ialah protocol pengangkutan yang membekalkan servis "datagram" pada bahagian teratas IP.

Terdapat dua protocol pengangkutan iaitu UDP dan TCP. Kedua-duanya bertanggungjawab untuk 2 program berkomunikasi antara satu sama lain, dimana IP bertanggungjawab dalam mendapatkan paket daripada mesin ke mesin menyeberangi internet. UDP, pada dasarnya hanya merupakan versi light-weight bagi TCP. Dimana, TCP secara automatiknya menghantar semula paket yang hilang, dimana ia tidak dihiraukan oleh UDP. Ini merupakan satu keuntungan untuk audio/visual, tetapi merupakan suatu kerugian untuk pertukaran fail.

Format UDP:





Port sumber mengenalpasti aplikasi pada mesin penghantar. Port destinasi mengenalpasti siapa yang menerima data. Jarak (length) menunjukkan kuantiti data di dalam paket. Checksum mengesahkan bahawa data yang dihantar tidak berubah semasa penghantaran dilakukan.

2.6.1.2 TCP (Transmission Control Protocol)

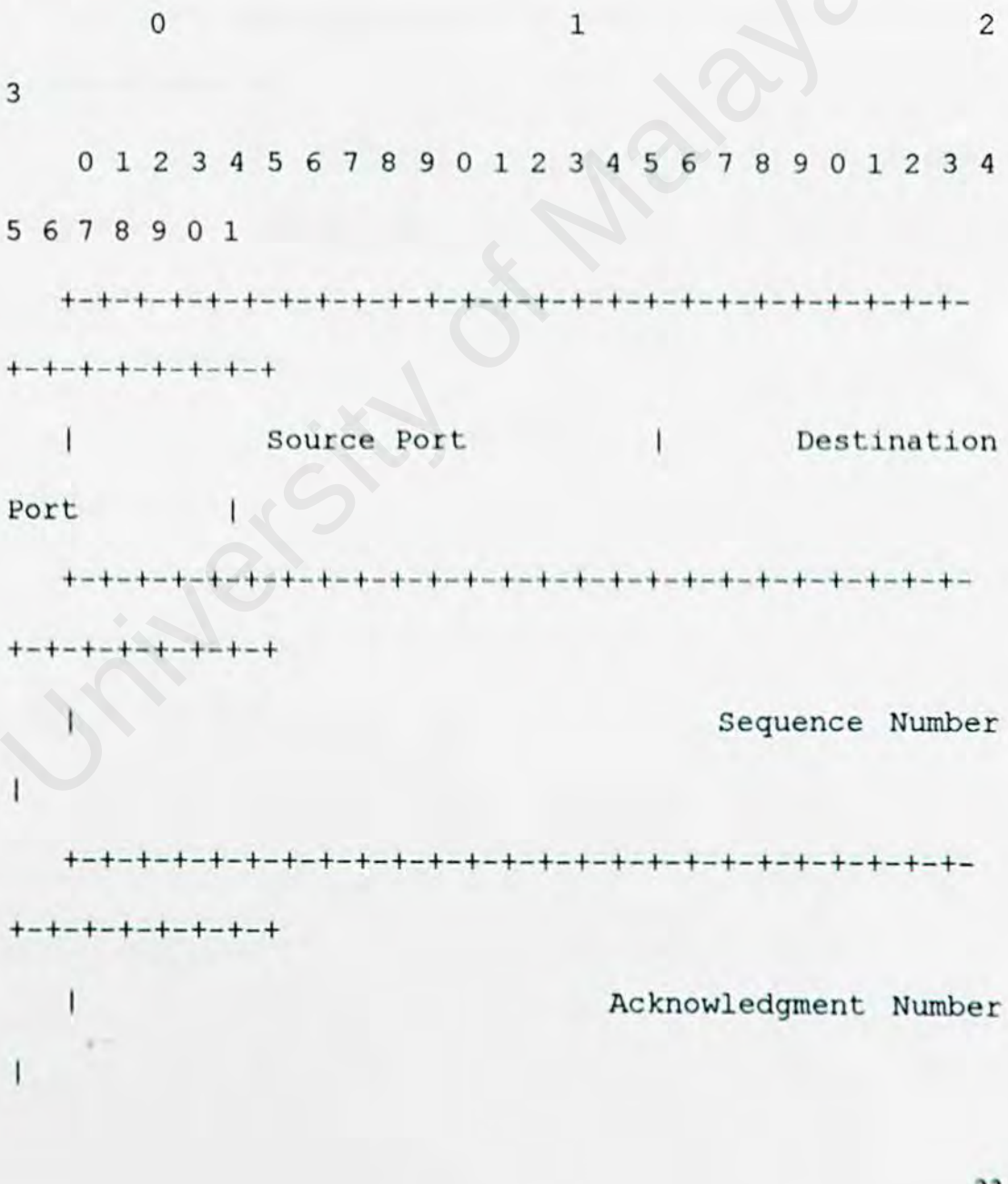
TCP berorientasikan sambungan . Ini bermakna data perlu dihantar melalui sambungan tersebut dengan pantas. Dengan ini penipuan alamat IP adalah mustahil tanpa ramalan siri nombor (sequence number prediction).

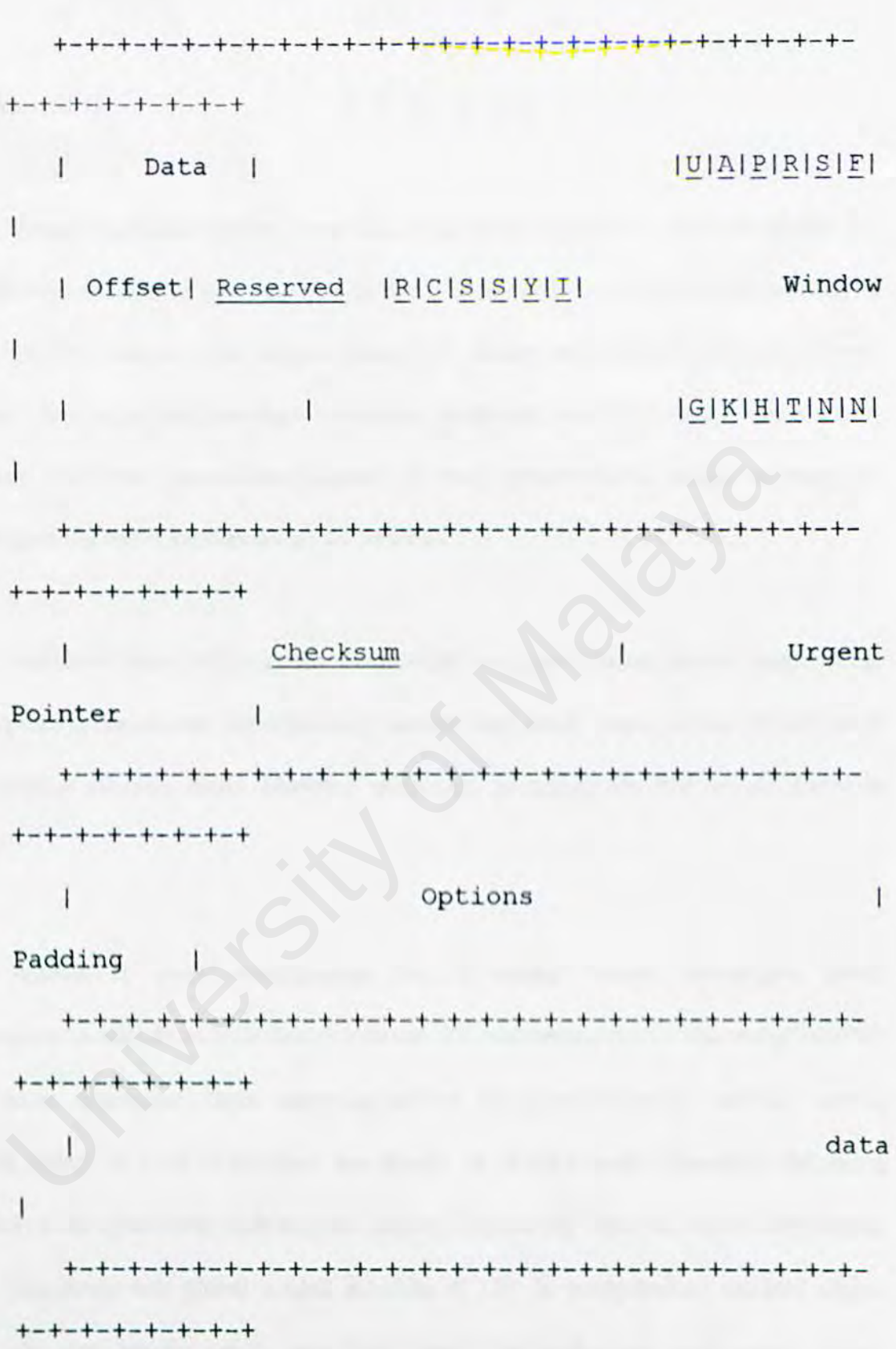
TCP mencipta sebuah jujukan bait maya untuk aplikasi. Oleh itu, aplikasi yang menghantar dan menerima data mesti mencipta sempadan mereka sendiri, seperti ukuran pengekodan data, atau menghantar teks data satu baris untuk satu masa. Bagaimanapun, aplikasi menghantar data dalam satu barisan yang lurus di dalam sempadan paket. Kebanyakan sistem pengesanan cerobohan berdasarkan rangkaian bergantung kepada sempadan ini untuk membolehkan ia menjalankan tugas dengan betul. Maka, mereka dengan mudahnya dapat dielak dengan "custom" penulisan skrip yang mana "misalign" data tersebut. Aplikasi tersebut tidak dapat melihat sebarang perubahan, dapat mengesan

sesuatu yang berlainan melalui wayar yang mana tidak lagi menyamai tandatangan mereka.

Terdapat dua protocol pengangkutan : TCP dan UDP. Dimana TCP berorientasikan sambungan manakala UDP tidak. Ini bermakna aplikasi dasar UDP mudah ditipu.

Format TCP:





2.6.2 Alamat IP

Dengan memiliki telefon, maka kita juga perlu mempunyai nombor telefon. Ini membolehkan sesiapa sahaja yang berada di mana-mana di seluruh dunia ini mendail ke telefon tersebut. Begitu juga dengan alamat IP, dimana apabila kita memiliki sebuah komputer dan ingin membuat capaian kepada rangkaian internet, atau apa-apa kategori rangkaian sekalipun, memerlukan alamat IP yang membolehkan pengguna-pengguna lain menghantar trafik kepada komputer tersebut.

Alamat IP dapat ditunjukkan secara tidak sengaja di dalam banyak komunikasi. Dengan memeriksa secara terperinci akan header bagi emel, maka alamat IP dari mana emel tersebut dihantar dapat diketahui, walaupun, pengguna tersebut berada disebalik firewall.

Alamat IP perlu ditempatkan dan dikekalkan secara berasingan dalam memastikan ia adalah unik di dalam internet. Ini bermakna apabila seseorang individu atau suatu organisasi ingin menyambungkan komputer-komputer mereka kepada internet, alamat IP perlu didaftarkan dan dengan ini ia tidak boleh digunakan oleh orang lain. Servis ini dibekalkan oleh banyak syarikat, seperti ISP (Internet Service Providers), tetapi tanggungjawab global adalah InterNic di US. Ia mengekalkan struktur alamat sedia ada, dan bekerja untuk yang baru kerana perkembangan penggunaan internet membuat jumlah alamat IP tidak lagi dapat menampung jumlah pengguna internet yang semakin meningkat dari hari ke hari.

2.6.3 Port

Di dalam TCP/IP, port merupakan sambungan bagi alamat internet yang memberitahu program yang mana yang akan menerima data. Contohnya, apabila kita menghantar data kepada 192.0.2.111, port 110, maka kita berinteraksi dengan POP3 servis emel. Bagaimanapun, jika kita menghantar data tersebut kepada port 80 pada mesin yang sama, sebenarnya kita berinteraksi dengan server web pada mesin tersebut.

Apabila saya memiliki dua URLs yang dilihat seakan sama http://afiatulsyahrizat.com:80/ dan http://afiatulsyahrizat.com:90/. Kedua-dua URLs ini membuat capaian pada server web yang berasingan tetapi program dilarikan pada mesin yang sama, satunya membuat capaian pada port 80 dan satu lagu pada port 90.

Ramai yang mempercayai bahawa port dapat mengenalpasti secara tepat akan protokol yang dilarikan pada port tersebut. Sebagai contoh, port 110 telah ditetapkan untuk POP3 servis emel. Walaupun port ini adalah betul bagi protocol, sesiapa sahaja dapat meletakkan servis yang berbeza untuk port ini, seperti HTTP. Sebagai contoh, URLs yang kelihatan seakan sama ialah HTTP://afiatulsyahrizat.com:110/

2.7 Soket/WinSock

Di dalam pengaturcaraan, antaramuka soket adalah cara yang biasa digunakan oleh pengekod untuk membuat capaian ke atas rangkaian. Soket bertindak dengan membuat satu "file handle" untuk menghantar data ke dalam rangkaian atau lebih tepat lagi ke dalam fail di dalam hard disk.

Antaramuka lain yang boleh digunakan oleh pengaturcara adalah pengasingan tahap lebih tinggi (higher level abstractions) seperti RPC, atau antaramuka pada tahap lebih rendah "raw" seperti libnet.

Soket, berasal daripada UNIX, tetapi telah dibawa kepada pelantaran yang lain. Winsock untuk Windows berbeza dimana ia turut memasukkan kedua-dua fungsi, iaitu fungsi UNIX dan fungsi Windows. Untuk menulis program soket asas adalah tidak mustahil yang mana ia dapat mengkompil kedua-dua pelantaran.

Soket diambil daripada perhubungan TCP/IP "socket". Soket merupakan maklumat minima yang perlu diketahui untuk komunikasi di dalam rangkaian: sumber / destinasi alamat IP., sumber / destinasi port, dan sumber / protocol pengangkutan (UDP tau TCP).

2.8 NDIS (Network Driver Interface Specification)

NDIS merupakan satu spesifikasi Windows untuk melihat bagaimana komunikasi program-program protocol seperti TCP/IP dan pemandu peranti rangkaian (network device driver) sepatutnya berkomunikasi antara satu sama lain. NDIS menentukan antaramuka untuk:

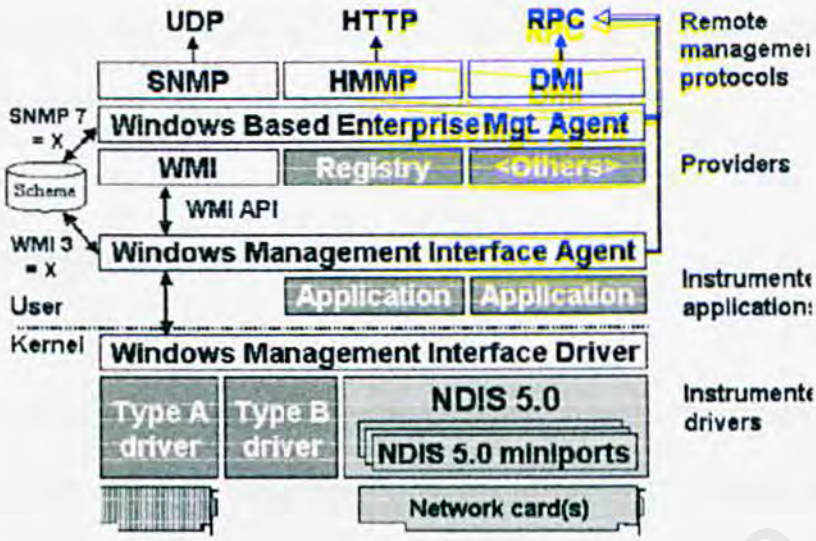
1. Program yang menghantar dan menerima data dengan membentuk atau mencabut ia daripada unit-unit yang telah diformat yang dinamakan lapisan protokol yang merupakan suatu lapisan dan secara generalnya adalah menyamai lapisan ke 3 dan ke 4 iaitu lapisan pengalamatan rangkaian dan lapisan pengangkutan di dalam model rujukan OSI (Open Systems Interconnection). Contohnya TCP/IP dan *Internetwork Packet Exchange*.

2. Program, yang selalunya disebut pemandu peranti (device driver), yang berhubung secara terus dengan kad antaramuka rangkaian (NIC) atau lain-lain *adapter* perkakasan yang menghantar atau menerima data di dalam talian komunikasi dalam bentuk isyarat elektronik. Pemandu program dan NIC berinteraksi pada sub lapisan alamat MAC (Media Access Control) iaitu pada lapisan ke 2 di dalam lapisan OSI (Data-Link Control). Meletakkan isyarat di dalam talian adalah di dalam lapisan pertama iaitu lapisan fizikal bagi lapisan OSI. Contoh pemandu MAC adalah Ethernet, *Fiber Distributed-Data Interface* (FDDI) dan *token ring*.

3. Suatu program yang dinamakan Pengurus Protokol yang membantu program *stack protocol* dan program pemandu MAC dengan memberitahu setiap satunya lokasi komputer lain apabila Sistem Pengendalian (Operating System) bermula atau dalam kes lain, bila perkakasan baru ditambah kepada komputer.

NDIS dibangunkan oleh Microsoft dan 3COM. Dengan menggunakan NDIS, Pembangun Perisian Windows boleh membina lapisan protokol yang dapat bekerja bersama pemandu MAC untuk mana-mana adapter komunikasi pembuat perkakasan. Dengan menggunakan token yang sama, apa-apa pembuat adapter boleh menulis perisian pemandu MAC yang juga boleh berkomunikasi dengan pelbagai program lapisan protokol.

Terdapat satu lagi antaramuka yang bersamaan dengan antaramuka ini, yang dinamakan *Open Data-Link Interface* (ODI). Antaramuka ini dibekalkan oleh Novell untuk system pengendalian Netware iaitu LAN mereka.



Rajah 2.1: Kedudukan suatu NDIS di dalam komputer

Walaubagaimanapun, di dalam membangunkan NaS ini, pemandu peranti rangkaian yang dipilih bertindak seperti NDIS dan ia berkeupayaan menangkap semua paket pengguna rangkaian bagi mendapatkan statistik penggunaan rangkaian. Pemandu peranti ini juga dipilih agar dapat menyokong mod campuran. Pemandu peranti yang akan digunakan adalah WinPcap yang akan dibincangkan dengan lebih lanjut lagi pada keperluan perisian di bab 3 (METODOLOGI).

2.9 Mod Campuran (Promiscuous Mode)

Adapter Ethernet yang biasa menolak semua trafik mendatang yang tidak dihantar kepada adapter itu. Untuk melakukan proses hiduan (sniff) pada wayar, adapter tersebut perlu dikonfigurasi semula agar dapat menerima semua trafik yang melalui wayar. Keadaan inilah yang dinamakan mod campuran. Sistem NaS yang dibangunkan

ini meyokong kehendak mod campuran. Diantara system yang turut mengaplikasikan mod ini ialah NIDS (Network Intrusion Detection System) dan Snort.

2.9.1 NIDS (Network Intrusion Dtection System)

NIDS merupakan satu sistem yang bertanggungjawab untuk mengesan data yang boleh dikategorikan sebagai data yang tidak dibenarkan berlaku di dalam rangkaian. Berlainan pula dengan *firewall*, dimana ia dikonfigurasikan untuk membenarkan atau menghalang capaian ke atas sesuati servis atau hos berdasarkan peraturan-peraturan yang telah ditetapkan. Jika trafik bersesuaian dengan *pattern*, maka ia diterima dengan tidak perlu menimbangkan kandungan paket tersebut. Walaubagaimanapun, NIDS menangkap dan memeriksa dengan teliti kesemua trafik, dengan tidak mempertimbangkan sama ada ia dibenarkan atau tidak.

2.9.1.1 Bagaimanakah NIDS menyesuaikan tandatangan dengan trafik yang mendatang?

Trafik terdiri daripada datagram IP yang melalui rangkaian. NIDS berkebolehan untuk menangkap paket-paket tersebut ketika mereka melalui rangkaian dengan melalui wayar. NIDS terdiri daripada longgokan TCP/IP yang menghimpunkan semula datagram IP dan aliran TCP. Ia memerlukan teknik-teknik berikut:

2.9.1.1(a) Pengesahan longgokan protocol

Bilangan cerobohan seperti "Ping-O-Death" dan "TCP Stealth Scanning" menggunakan perlanggaran lapisan bawah IP, TCP, UDP, dan protocol ICMP untuk menyerang mesin tersebut. Sistem pengesahan yang mudah boleh melemahkan (flag) paket yang tidak sah. Ia juga boleh kadangkala sah, dengan perlakuan curiga seperti dengan kadangkala memecahkan paket IP.

2.9.1.1(b) Pengesahan protocol aplikasi

Suatu bilangan cerobohan yang menggunakan perlakuan protocol yang tidak sah seperti "WinNuke", yang menggunakan protocol NetBIOS yang tidak sah (menambah data OOB) atau cache DNS yang beracun, dimana ianya sah, tetapi bukan tandatangan yang biasanya. Bagi mengesan pencerobohan ini secara efektif, NIDS mesti membentuk semula kepelbagaian protocol pada lapisan aplikasi. Ini adalah untuk mengesan perlakuan yang mencurigakan atau tidak sah.

2.9.1.1(c) Membuat acara baru yang boleh log

Suatu NIDS bolch digunakan untuk memanjangkan kebolchan untuk mengaudit perisian pengurusan rangkaian. Sebagai contoh, suatu NIDS boleh log kesemua protokol lapisan aplikasi yang digunakan pada mesin.

2.9.2 Snort

Kini Snort semakin dikenali ramai dan digemari oleh ramai. Ia memiliki lebih 100 tandatangan sendiri dan pengguna lain yang boleh didapati melalui internet.

Dibawah merupakan salah satu contohnya:

```
# here's an example of PHF attack detection where just a straight text string
# is searched for in the app layer
alert tcp any any -> 192.168.1.0/24 80 (msg:"PHF attempt"; content:"/ cgi-bin/phf";)
```

Ia menyatakan supaya memberikan amaran pada sambungan TCP daripada mana-mana alamat IP dan mana-mana port kepada 192.168.1.x subnet kepada port 80. Ia mencari "/cgi-bin/phf" tidak kira dimana ia berada di dalam kandungan tersebut. Jika kandungan seperti ini diketemu, amaran akan diberikan kepada konsul dengan mesej "PHF attempt".

Penggunaan Snort selalunya dilakukan dengan cara berikut:

- Penapis BPF (bahagian bagi libcap) dikonfigurasikan untuk difokuskan kepada jenis-jenis trafik tertentu.

- Keputusan dibuat berdasarkan alamat IP mana adalah luaran dan yang mana adalah dalaman bagi menambahkan lagi pemfokusan.

- Peraturan digubah bagi memuatkan persekitaran tempatan / dalaman.
- Larian system.

- Peraturan digubah lagi untuk menyingkirkan kesalahan-kesalahan yang berlaku.

Snort juga mempunyai bilangan pilihan yang boleh digunakan untuk menghidu trafik rangkaian.

2.10 Banding Beza antara beberapa Pangkalan Data

Bahagian ini menerangkan perbandingan di antara beberapa pangkalan data. Bagaimanapun pangkalan data yang dipilih untuk membangunkan sistem ini, akan diterangkan pada bahagian keperluan perisian di dalam bab 3.

2.10.1 Server Microsoft SQL 7.0

Server Microsoft SQL 7.0 merupakan system yang fleksibel, memberikan kesesuaian terhadap perkakasan, mudah disesuaikan dengan penggunaan muatan yang tinggi dan kuantiti maklumat yang banyak. Ia juga bersepaduan dengan sistem pengendalian. Server SQL ini juga merupakan servis yang sebenar, dimana ia dapat melarikan sebagai latar belakang tugas pada server dan juga dapat mengendalikan permintaan untuk data dari ramai pengguna.

Server Microsoft SQL 7.0 ini menyokong beberapa ciri-ciri yang menghasilkan faedah-faedah berikut:

- *Kemudahan untuk pemasangan, pembahagian, dan penggunaan.* Server SQL juga terdiri daripada satu set alatan pentadbiran dan pembangunan yang dapat meningkatkan kebolehan untuk memasang, membahagi, mengurus dan menggunakan server SQL.

- *Scalability.* Pangkalan Data ini dapat digunakan pada komputer-komputer, daripada laptop yang melarikan Microsoft Windows 95 / 98 dan ke atas, sehinggalah server multipemproses yang melarikan Microsoft Windows NT.
- *Gudang Data.* Server SQL juga melibatkan alatan untuk memecahkan dan menganalisa data ringkas untuk OLAP (online analytical processing). Server SQL juga melibatkan alatan yang digunakan untuk mereka bentuk pangkalan data secara visual dan menganalisa data menggunakan soalan berasaskan Bahasa Inggeris.
- *Penyatuan Sistem dengan perisian server lain.* Server SQL ini juga disepadukan dengan emel, internet dan windows.

2.10.2 Oracle

Oracle adalah lebih mahal daripada Access, Informix, Sybase, dan beberapa Server SQL. Ia memiliki senibina server pelbagai talian yang mengkoordinasikan ribuan permintaan pengguna secara serentak. Ini membenarkan penggunaan ingatan yang efisyen. Dengan itu, Oracle dapat menyokong pangkalan data yang lebih besar dan lebih selamat daripada server-server pangkalan data yang lain.

Tambahan lagi, Oracle menggunakan model data berkaitan, yang menawarkan kelebihan-kelebihan berikut untuk mencapai maklumat yang tersimpan.

- Struktur data dan bahasa data yang ringkas
- Kesemua jenis-jenis perkaitan dapat dipersembahkan semula dengan mudah.

- Darjah kebebasan data yang tinggi
- Meningkatkan kemudahcapaian bagi capaian ad hoc.
- Penyelenggaraan bagi pangkalan data berkaitan adalah ringkas dan lebih murah daripada model data lain.

2.10.3 MySQL

MySQL merupakan pangkalan data berkaitan yang kecil dan berkebolehan. Ia juga merupakan perisian sumber terbuka. Ini bermakna adalah mudah bagi sesiapa yang ingin mengubah perisian ini. Kod sumber juga sedia ada untuk umum. Sesiapa sahaja dapat mempelajari kod sumber ini dan menukarkan ia bagi memenuhi kehendak mereka.

MySQL merupakan system klien / server yang memuatkan pelbagai talian server SQL yang menyokong beberapa program klien dan perpustakaan yang berbeza, alatan pentadbiran dan antaramuka pengaturcaraan. Ianya juga adalah dianggap sangat pantas, berkebolehan dan mudah digunakan. MySQL juga memiliki ciri-ciri yang praktikal dan dibangunkan di dalam persekitaran kerjasama yang rapat dengan penggunanya.

MySQL dibina untuk mengawal pangkalan data yang sangat besar, lebih pantas daripada pangkalan data sedia ada. Ia berjaya digunakan di dalam persekitaran yang sangat mementingkan pengeluaran untuk beberapa tahun. Bagaimanapun, di bawah pembangunan yang berterusan, pada hari ini, MySQL menawarkan fungsi-fungsi yang yang berguna. Kadar harga yang rendah dan fleksibel yang ditawarkan kepada pengguna

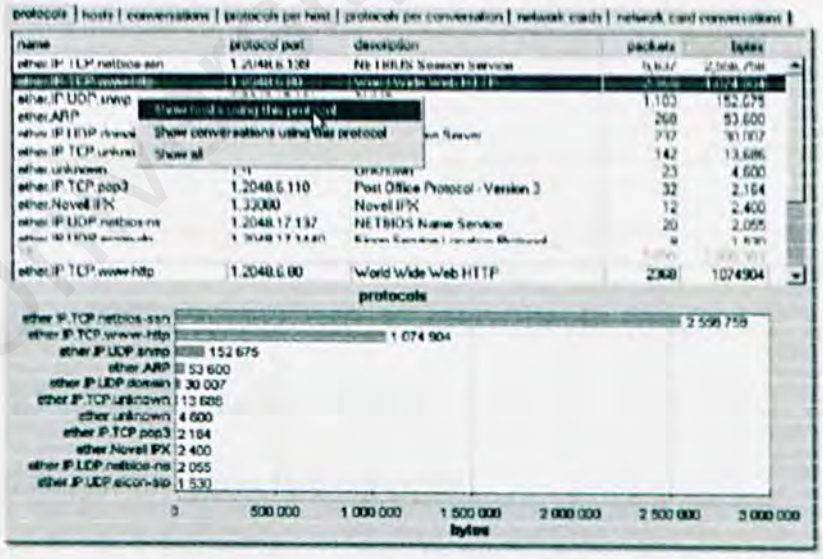
dan pembangun-pembangun system, ditambah dengan kelajuan sambungannya dan keselamatan, membuat MySQL bertambah dikenali ramai.

2.11 Sistem yang berkaitan ("Network Probe")

Sistem ini merupakan suatu jenis sistem pemantauan rangkaian dan penganalisa protokol yang dapat memberikan gambaran situasi trafik di dalam rangkaian.

Semua trafik dipantau di dalam masa nyata dan dipaparkan kepada pengguna sebagai kombinasi diantara carta dan jadual, memberikan maklumat secara terperinci tentang hos dan protokol, sebagai paparan bagi situasi trafik di di dalam rangkaian.

Melalui system ini, maklumat dapat dapat dicari, dibahagikan, dan ditapis oleh protokol, hos, perbualan, dan antaramuka rangkaian.



Rajah 2.2 : Gambarajah Sistem "Network Probe"

2.11.1 Ciri-ciri "Network Probe":

- Menapis protokol terpilih
- Menapis hos terpilih
- Menapis perbualan terpilih
- Melihat di dalam masa nyata, protokol, hos yang aktif, perbualan, statistik protokol terperinci bagi setiap hos dan setiap perbualan, juga kad rangkaian secara terperinci.

2.11.2 Keperluan Sistem

Sistem "Network Probe ini diaturcarakan di dalam bahasa pengaturcaraan Java dan berasaskan server klien di mana server dilarikan pada satu mesin dan mendapatkan statistik bagi trafik rangkaian, klien yang di larikan menggunakan java membolehkan web browser pada mesin yg lain..

Server "Network Probe"

- Windows NT, Windows 2000, Windows XP atau Linux/Unix
- Java 1.1.8 runtime or later installed
- Kad rangkaian dengan mod campuran

- Internet Explorer, Netscape, atau Opera dengan Java.

2.11.3 Kekurangan sistem "Network Probe" berbanding "NaS"

- Makumat yang diambil daripada proses penapisan disimpan di dalam "text file", sementara untuk NaS, maklumat tersebut disimpan di dalam pangkalan data.

- Tidak membekalkan katalaluan kepada penggunanya.

BAB 3 : METODOLOGI DAN ANALISA SISTEM

3.1 Pengenalan

Fasa metodologi dan analisis sistem bertujuan untuk mengenalpasti keperluan fungsian dan bukan fungsian bagi sistem yang bakal dibangunkan. Dalam usaha untuk membangunkan Sistem Penganalisa Rangkaian (NAs), beberapa pendekatan telah dianalisis dan dikaji bagi memastikan keperluan sistem dipenuhi sepenuhnya bagi menghasilkan produk yang baik.

Setelah membuat kajian terhadap beberapa pendekatan yang boleh digunakan sebagai alatan untuk membangunkan sistem, maka pendekatan model Air Terjun dirasakan sebagai satu pilihan yang tepat. Model Air Terjun ini walaubagaimanapun merupakan model yang telah diubahsuai dan ianya digunakan memandangkan ia merupakan model yang berjujukan, sistematik dan mempunyai ciri-ciri kitaran yang sangat berguna dalam pembangunan sistem.

Melalui model ini, proses pembangunan dari satu fasa ke satu fasa seterusnya adalah jelas dan sekiranya berlaku kesilapan dalam sesuatu fasa, ianya boleh diperbetulkan semula tanpa perlu menanti fasa seterusnya siap. Selain itu, model ini juga sering menjadi pilihan pembangun-pembangun sistem. Walaubagaimanapun, sebelum diterangkan dengan lebih lanjut lagi berkenaan dengan model Air Terjun ini, akan diterangkan secara ringkas terlebih dahulu berkenaan dengan Kitar Hayat Pembangunan

Sistem (SDLC). Dengan penerangan ini, diharap gambaran dapat diberikan bagi membolehkan model Air Terjun difahami secara kasar.

3.2 Kitar Hayat Pembangunan Sistem (SDLC-System Development Life Cycle)

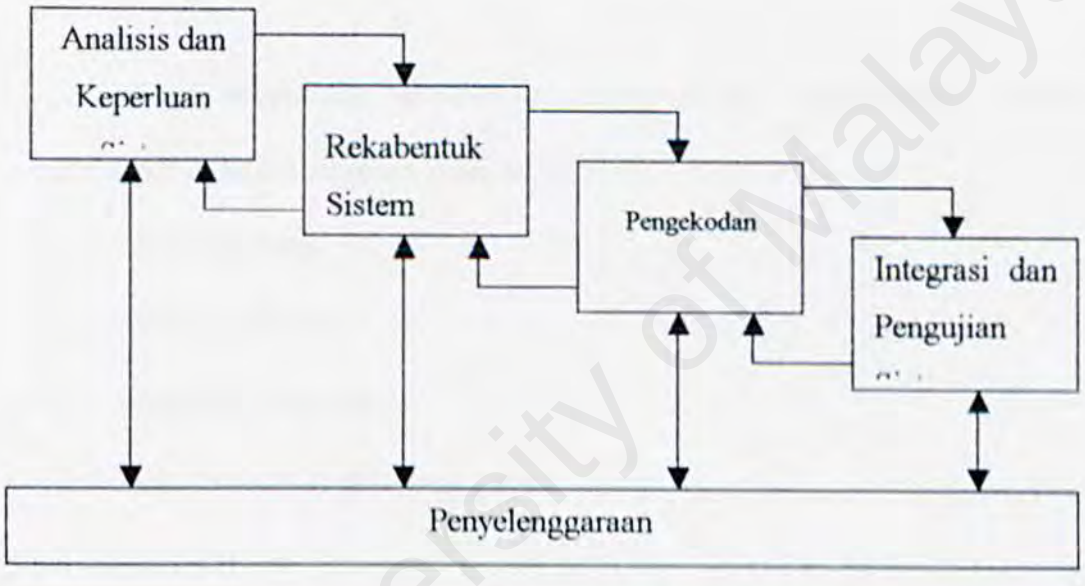
Kitar Hayat Pembangunan Sistem atau SDLC ini merupakan satu fasa yang menghampiri kepada Analisis dan Rekabentuk Sistem, dimana ia menerangkan bahawa suatu sistem dapat dibangunkan dengan baik dengan penggunaan kitaran yang khusus bagi penganalisa dan aktiviti-aktiviti pengguna.

Pada umumnya, SDLC dibahagi kepada 7 fasa. Walaupun setiap fasa dipaparkan secara senyap, ia tidak pernah disempurnakan sebagai langkah yang berasingan. Sebaliknya, beberapa aktiviti boleh berlaku secara serentak, dan aktiviti-aktiviti boleh diulangi. 7 fasa tersebut adalah:

i. Mengenalpasti masalah, peluang, dan objektif.
ii. Mengambilkira maklumat dan permintaan.
iii. Menganalisa keperluan sistem.
iv. Merekabentuk sistem yang disarankan.
v. Membangun dan mendokumenkan perisian.
vi. Menguji dan menyelenggara sistem.
vii. Melaksana dan menilai sistem.

Walaubagaimanapun, SDLC mempunyai beberapa kelemahan. Ianya memakan masa yang terlalu panjang dan ini memanjangkan masa bagi pembangunan sistem. Berikutan dengan ini, SDLC memakan kos yang agak tinggi untuk dilaksanakan. Oleh yang demikian, model Air Terjun adalah lebih sesuai untuk pembangunan proses bagi Sistem Penganalisa Rangkaian ini.

3.3 Model Air Terjun



Rajah 3.1: Model Air Terjun

3.3.1 Analisis dan Keperluan Sistem

Proses pengumpulan keperluan dititikberatkan dan diberikan penekanan utama. Kerja-kerja membangun sistem dimulakan dengan mengumpulkan keperluan untuk semua elemen sistem dan membandingkan maklumat dan operasinya untuk meningkatkan kualiti sistem yang akan dibangunkan.

3.3.2 Rekabentuk Sistem

Fasa rekabentuk melibatkan proses-proses merekabentuk sistem dan ia melibatkan 4 atribut program nyata iaitu:

1. Struktur Data
2. Senibina Perisian
3. Prosedur Terperinci
4. Ciri-ciri antaramuka pengguna

Proses Rekabentuk menterjemahkan keperluan ke dalam bentuk persembahan perisian yang boleh dicapai untuk kualiti sebelum proses pengekodan bermula. Seperti keperluan rekabentuk didokumentasikan dan menjadi sebahagian daripada konfigurasi perisian.

3.3.3 Pengekodan

Rekabentuk perlu diterjemahkan ke dalam bentuk yang boleh dibaca oleh mesin. Proses pengekodan melaksanakan tugas-tugas ini. Jika rekabentuk dipersembahkan dalam keadaan terperinci, fasa pengekodan boleh disempurnakan dengan jayanya.

3.3.4 Integrasi dan Pengujian Sistem

Setelah kod dijanakan, proses pengujian bermula. Proses pengujian memfokuskan logikal dalaman suatu perisian, memastikan kesemua pernyataan telah diuji ke atas fungsian luaran, mengarahkan ujian untuk tidak melakukan kesilapan dan memastikan input yang ditakrif akan menghasilkan keputusan sebenar.

3.3.5 Penyelenggaraan

Sistem akan mengalami perubahan jika ia tidak memenuhi isyarat seperti yang dipinta. Perubahan berlaku kerana kesilapan telah ditemui memandangkan sistem perlu disesuaikan dengan perubahan pada persekitaran luaran. Penyelenggaraan sistem perlu dilakukan agar sistem dapat dilarikan dengan sempurna.

3.4 Kenapa memilih Model Air Terjun?

Model Air Terjun dipilih sebagai model proses pembangunan bagi Sistem Penganalisa Rangkaian adalah disebabkan oleh sebab-sebab yang disenaraikan di bawah:

- Kaedah ini merupakan salah satu daripada kaedah yang paling banyak digunakan di dalam suatu proses pembangunan sistem. Ia juga mudah difahami dan dilaksanakan di dalam proses pembangunan bagi suatu sistem.

- Proses pembangunan bagi model Air Terjun ini adalah berterusan merujuk kepada fasa yang telah dipilih.

- Model Air Terjun ini menyokong jarak penglihatan proses dimana setiap aktiviti menghasilkan suatu penghantaran. Penghantaran ini boleh dibuktikan berguna apabila sistem berkembang pada masa akan datang.

- Model Air Terjun ini diberikan pendekatan berperaturan untuk membangunkan sebuah sistem sebagai persediaan dokumen selepas setiap peringkat perlu diperiksa dan disahkan.

- Model ini membolehkan penyelenggaraan dibawa keluar pada setiap peringkat bagi mengulangi peringkat sebelumnya, mengikut kehendak semasa. Perubahan boleh dilakukan pada setiap peringkat dengan kembali kepada peringkat sebelumnya. Proses ulang semula ini, boleh dibawa keluar seberapa banyak kali yang perlu dan ini menghasilkan sebuah sistem akhir yang berkualiti tinggi yang mana memenuhi kehendak pengguna.

BAB 4 : ANALISA SISTEM

4.1 Pengenalan

Fasa analisis sistem bertujuan untuk mengenalpasti keperluan fungsian dan bukan fungsian bagi sistem yang bakal dibangunkan. Dalam usaha untuk membangunkan Sistem Penganalisa Rangkaian (NAs), beberapa pendekatan telah dianalisis dan dikaji bagi memastikan keperluan sistem dipenuhi sepenuhnya bagi menghasilkan produk yang baik.

4.2 Pendekatan Kajian

Pelbagai pendekatan dijalankan telah diambil dalam membuat kajian terhadap aspek-aspek berkaitan dan telah mensasarkan kepada pencarian lebih lagi fakta-fakta di dalam merekabentuk NAs. Maklumat yang didapati melalui proses ini akan diaplikasikan di dalam pembangunan NAs.

4.2.1 Buku Rujukan

Buku-buku rujukan yang digunakan adalah berkaitan dengan suatu persekitaran rangkaian, pangkalan data, bahasa pengaturcaraan dan lain-lain yang mempunyai pendekatan dengan pembangunan projek.

4.2.2 Enjin Pencarian

Enjin pencarian telah digunakan untuk mempermudahkan pencarian maklumat. Di antara enjin pencarian yang digunakan adalah AltaVista, Yahoo, Google, dan Catcha. Enjin pencarian ini dapat memulangkan keputusan yang berguna untuk projek yang dibangunkan. Katakunci yang digunakan di dalam membuat pencarian ini adalah seperti "Network Intrusion Detection System", Snort, Waterfall model, dan banyak lagi.

4.2.3 Tesis yang sedia ada

Laporan latihan ilmiah yang disediakan oleh pelajar-pelajar sebelum ini juga merupakan satu lagi sumber rujukan yang digunakan. Laporan latihan ilmiah ini boleh didapati di dalam bilik dokumen fakulti. Laporan-laporan tersebut disediakan sebagai panduan yang berguna terutama sekali di dalam proses menyediakan laporan ini.

4.2.4 Lain-lain

Sumber maklumat lain yang digunakan untuk proses menyediakan laporan ini adalah seperti majalah-majalah, dan surat khabar.

4.3 Analisis Keperluan

Keperluan perlu dikenalpasti dan seterusnya ia perlu di analisis dan diklasifikasikan. Terdapat 2 jenis keperluan yang perlu di analisis iaitu keperluan fungsian dan keperluan bukan fungsian.

4.3.1 Keperluan Fungsian

Keperluan fungsian menyatakan dan menunjukkan apa yang perlu dilakukan oleh suatu sistem yang baru. Keperluan fungsian ialah fungsi-fungsi yang diperlukan untuk melengkapkan sistem. Dengan adanya fungsi-fungsi ini, NAs akan dapat dilaksanakan dengan sepenuhnya. Keperluan fungsian ini telah dibahagikan kepada 4 bahagian utama iaitu:

1. Penangkapan paket data
2. Penapisan data
3. Analisis Protokol
4. Pengeluaran hasilan

4.3.1.1 Penangkapan paket data

Penangkapan paket data ialah proses dimana salinan dibuat ke atas paket-paket data yang melalui wayar rangkaian. Salinan yang dibuat adalah daripada paket-paket data bagi yang menyeberangi wayar rangkaian. Kaedah "wiretapping" yang mengaplikasikan mod campuran (promicious mode) digunakan bagi menangkap paket-paket data tersebut.

4.3.1.2 Penapisan data

Penapisan data ialah keadaan di mana paket-paket data yang telah di tangkap, di pilih dan di bahagikan kepada bahagian-bahagiannya. Data-data yang tidak diperlukan tidak diambil. Pembahagian-pembahagian ke atas paket dasar tersebut adalah berdasarkan jenis alamat IP, jenis port, dan jenis protokolnya.

4.3.1.3 Analisis Protokol

Analisis protokol merupakan proses dimana paket-paket data yang telah di tapis, di analisa, untuk mendapatkan statistik setiap satu bahagiannya.

4.3.1.4 Pengeluaran hasilan

Pengeluaran hasilan akan dihantar kepada 2 bahagian iaitu hasilan yang akan di simpan ke dalam pangkalan data dan dipaparkan kepada skrin komputer.

4.3.2 Keperluan Bukan Fungsian

Keperluan bukan fungsian adalah keperluan yang menakrifkan keupayaan dan kekangan sistem. Keperluan bukan fungsian diperlukan dalam melaksanakan operasi dan piawaian perisian. Antara keperluan bukan fungsian bagi sistem ini termasuklah:

4.3.2.1 Ketahanan / kekekalan

Ketahanan merupakan suatu darjah bagi sistem supaya mudah di kekalkan dan efektif. Ini dapat memastikan pengubahsuaian kepada fungsi tidak akan mengurangkan keberkesanan prestasi sistem tersebut. Sistem ini juga mudah diubahsuai dan di uji dalam meningkatkan tahap proses agar dapat menjalankan permintaan-permintaan terkini., membetulkan kesalahan, atau pada sistem komputer yang lain.

4.3.2.2 Kebolehpercayaan

Kebolehpercayaan ialah di mana sistem dapat mempersembahkan prestasinya di dalam cara yang betul dan memproses ia mengikut kehendak rekabentuknya.

4.3.2.3 Kecekapan

Perlaksanaan sistem adalah sejajar dengan banyak kos. Penggunaan sumber komputer yang cekap di mana setiap proses dapat dilaksanakan dengan tersusun dan teratur dan membawa kepada perlaksanaan yang sempurna. Perkakasan dan perisian juga perlu digunakan secara cekap bagi mencapai prestasi yang mantap.

4.3.2.4 Mesra Pengguna

Sistem ini memerlukan antaramuka yang mudah digunakan. Ia perlu direkabentuk untuk memaparkan maklumat yang perlu untuk penggunanya. Secara amnya, rekabentuk sistem ini perlu mempunyai kriteria-kriteria berikut:

- Konsisten dalam rekabentuk antaramukanya, dan dapat memaparkan mesej kesilapan.
- Mempunyai darjah kefahaman yang tinggi.

4.3.2.5 Kebolehgunaan

Sistem ini perlu digunakan oleh penggunanya tanpa memberi banyak kesulitan kepada penggunanya. Ia perlu membantu pengguna dalam menggunakan perisian tersebut.

4.3.2.6 Kemantapan Prestasi

Sistem perlu mempersembahkan prestasi yang baik, walaupun telah digunakan terlalu kerap. Ia perlu sekurang-kurangnya mempersembahkan muatan tugas yang berat apabila menyediakan tugas yang banyak pada masa yang sama.

4.4 Penggunaan teknologi dalam pembangunan sistem

Pemilihan perkakasan dan perisian adalah sangat penting dan sukar dilakukan oleh mereka yang belum mempunyai pengalaman di dalam pembangunan sesebuah aplikasi. Perkakasan dan perisian yang dipilih mestilah bersesuaian dan bertepatan dengan keperluan aplikasi yang akan dibangunkan. Ini adalah penting bagi memastikan aplikasi berjaya dibangunkan. Pemilihan hendaklah dibuat dengan teliti supaya proses pembangunan dapat berjalan dengan lancar dan memenuhi kehendak aplikasi yang ingin dibangunkan. Dalam pemilihan perkakasan dan perisian, faktor-faktor berikut perlu diambil kira, iaitu:

- Adakah perkakasan dan perisian mudah diperolehi serta biasa digunakan?
- Kos yang diperlukan untuk mendapatkan perkakasan dan perisian tersebut.
- Adakah spesifikasi perkakasan dan perisian sesuai dengan aplikasi yang hendak dibangunkan.

4.4.1 Keperluan Perkakasan

- Komputer peribadi IBM dan bersesuaian
- Pemproses mikro, sekurang-kurangnya 233Mhz
- RAM, sekurang-kurangnya 32Mb
- Ruangan storan, sekurang-kurangnya 10Mb cakera keras.
- Monitor, sekurang-kurangnya, 800x600 pixel
- Peranti input, papan kekunci dan tetikus

4.4.2 Keperluan Perisian

4.4.2.1 Microsoft Visual BASIC

Visual C++ dipilih sebagai bahasa pengaturcaraan yang akan digunakan untuk membangunkan sistem ini. Diantara keistimewaan bahasa pengaturcaraan ini adalah:

i. Ia berasaskan antaramuka pengguna bergrafik (GUI).

ii. Boleh diintegrasikan di dalam pangkalan data seperti Ms Access, Ms Foxpro dan Paradox

iii. Kesesuaiannya dengan perisian Windows

iv. Menyokong ODBC (Open Database Connectivity) yang membolehkan capaian kepada pelayan-pelayan dan pangkalan-pangkalan data tempatan termasuk SQL-server, SybaseSQL, dan Oracle.

v. Menggunakan konsep pengaturcaraan bermodul, dan pengesanan ralat mudah dengan memfokuskan kepada modul yang bermasalah sahaja. Modul-modul lain boleh dilarikan tanpa masalah.

4.4.2.2 Microsoft Access 2000

Microsoft merupakan salah satu perisian yang boleh menyokong penggunaan pangkalan data. Microsoft Access boleh digunakan sebagai pangkalan data pada pelayan atau berbilang senibina sistem. Ia menyediakan antaramuka mesra pengguna supaya dapat membina pangkalan data dengan mudah. Ia mempunyai beberapa versi, dan versi yang akan digunakan untk membangunkan system ini adalah dari versi Microsoft Access 2000. Perisian ini mempunyai ciri-ciri baru yang terkini dan bersesuaian dengan perkembangan teknologi perisian.

Melalui Microsoft Access 2000, pembangunan sistem tidak mengalami masalah dalam menambah atau menghapuskan data kerana ia boleh dilakukan terus di dalam pangkalan data tanpa melibatkan bahagian pengaturcaraan. Antara sebab-sebab yang menjadikan pangkalan data ini digunakan untuk membangunkan Sistem Penganalisa Rangkaian ini termasuk:

- Penciptaan rekod-rekod medan adalah lebih cepat berbanding dengan penciptaan menggunakan kod.
- Jenis data boleh dispesifikasikan denagn mudah.

- Perhubungan di antara rekod boleh dicipta dengan mudah.
- Lebih mudah untuk melihat serta memperbaiki ralat yang timbul.
- Ia bersifat multi pengguna.
- Sesuai dengan aplikasi sistem.

4.4.2.3 WinPcap

WinPcap merupakan senibina untuk penangkapan paket dan analisis rangkaian yang akan digunakan dalam membangunkan sistem ini. Ia turut termasuk penapisan paket pada lapisan-kernel, tahap rendah talian perpustakaan dinamik, dan tahap tinggi untuk sistem perpustakaan bebas.

Penapis paket merupakan peranti pemandu yang ditambah kepada windows 95, 98, ME, NT, 2000, dan XP. Ia mempunyai keupayaan untuk menangkap jujukan data daripada kad antaramuka rangkaian, dengan kebolehan menapis dan menyimpan paket yang ditangkap itu, ke dalam penimbal.

"Packet.dll" merupakan API dimana, ia boleh digunakan untuk capaian terus ke atas fungsi pemandu peranti, dan menawarkan satu program antaramuka yang bebas daripada sistem pengendalian Microsoft.

WinPcap.dll menghantar suatu set tangkapan primitif tahap tinggi yang bersesuaian dengan libpcap. Fungsi ini membenarkan untuk tangkapan paket di dalam cara bebas, daripada perkakasan rangkaian dan sistem pengendalian.

4.4.2.4 Sistem Pengendalian

Untuk Sistem Penganalisa Rangkaian ini, dapat menyokong semua sistem pengendalian bagi windows yang lebih tinggi daripada windows 98. Oleh itu sistem pengendalian yang dapat menyokong sistem ini termasuklah Win 98, Win Nt 4.0, Win 2000, Win XP, dan Win Me.

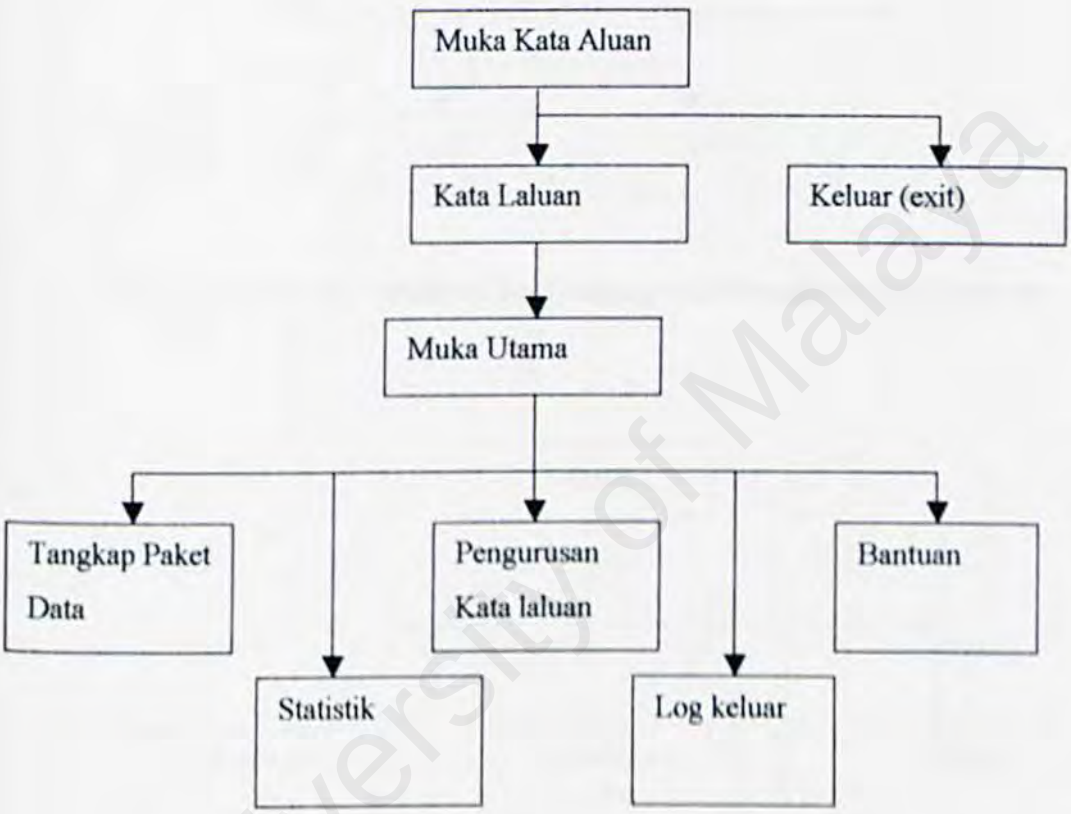
BAB 5 : REKABENTUK SISTEM

5.1 Pengenalan

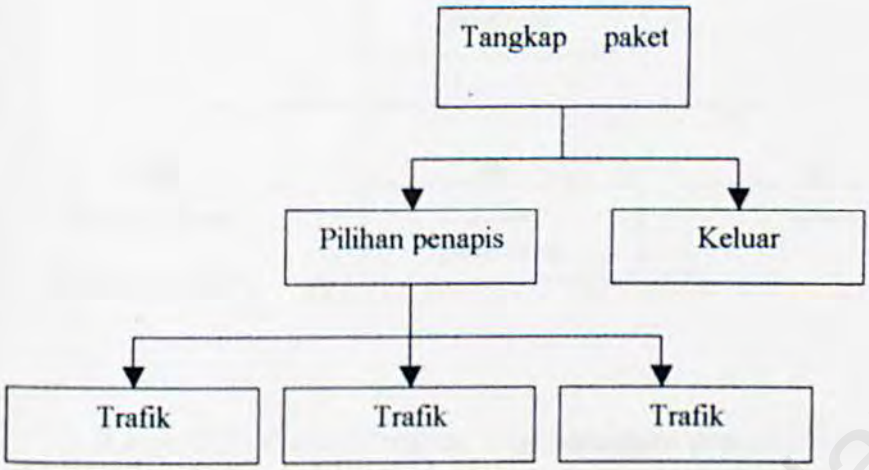
Rekabentuk sistem merupakan proses yang menerang, mengatur, dan menyusun rangka komponen bagi sistem untuk senibina secara terperinci yang membolehkan sistem yang dicadangkan ini dibangunkan. Idea penting adalah penerangan rekabentuk, pengurusan, dan struktur yang memfokuskan kepada pembinaan sistem baru. Rekabentuk sistem adalah seperti suatu set pelan yang diperlukan untuk membina sebuah rumah. Pelan tersebut di aturkan oleh komponen-komponen rumah yang berbeza dan menerangkan tentang bilik, dinding, dan lain-lain secara terperinci. Begitu juga di dalam rekabentuk sistem ini, walaupun komponen-komponennya adalah daripada komponen sistem baru. Rekabentuk sistem juga merupakan salah satu daripada fasa di dalam pembangunan sistem dimana keperluan sistem diterjemah ke dalam ciri-ciri sistem.

5.2 Carta struktur proses

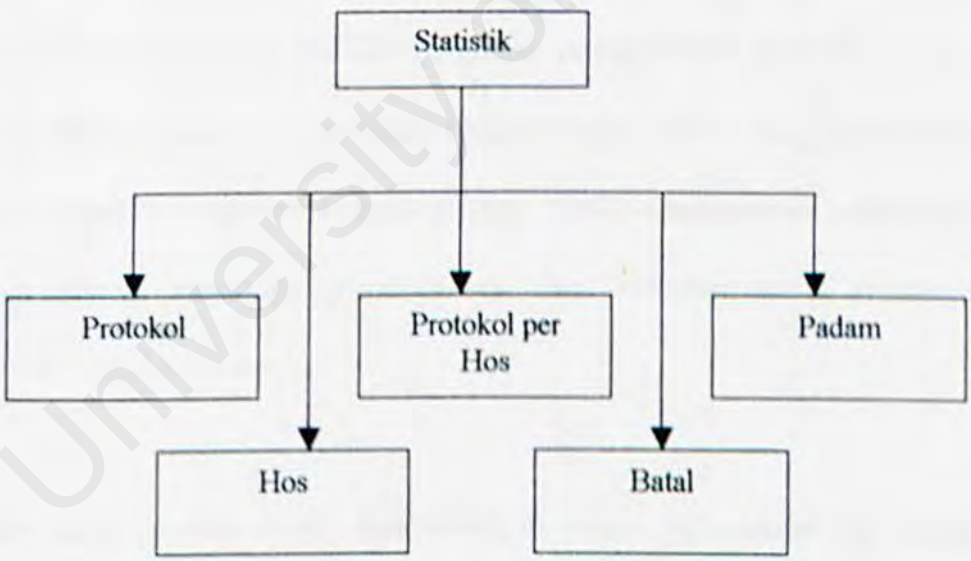
Carta struktur menunjukkan pengabstrakan peringkat tinggi di dalam spefikasi sistem. Carta ini digunakan untuk menerangkan komponen-komponen yang terdapat di dalam sistem.



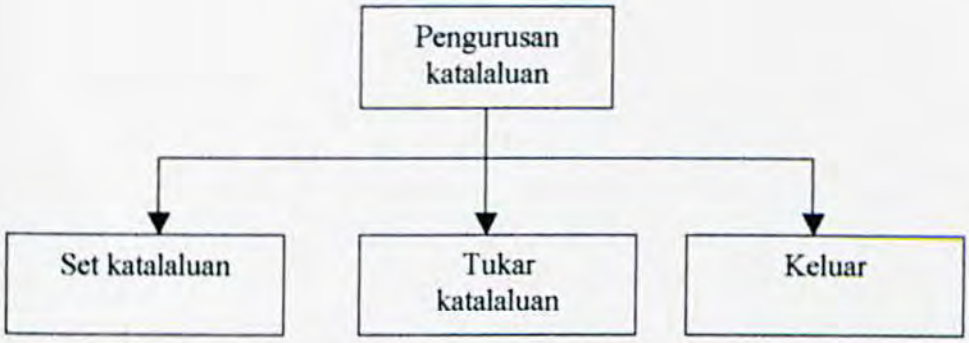
Rajah 5.1 : Carta struktur utama Sistem Penganalisa Rangkaian



Rajah 5.2 : Carta struktur bagi bahagian penangkapan paket data



Rajah 5.3 : Carta struktur bagi bahagian statistik

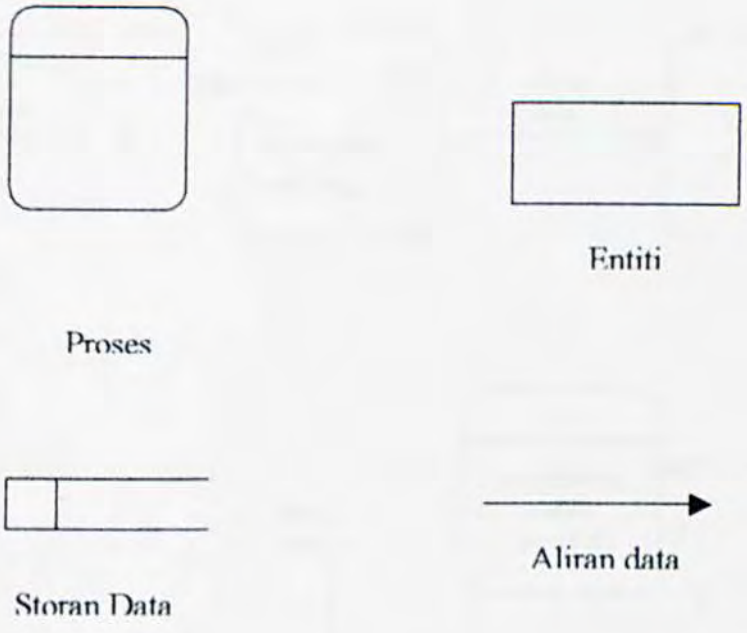


Rajah 5.4 : Carta struktur bagi bahagian pengurusan katalaluan

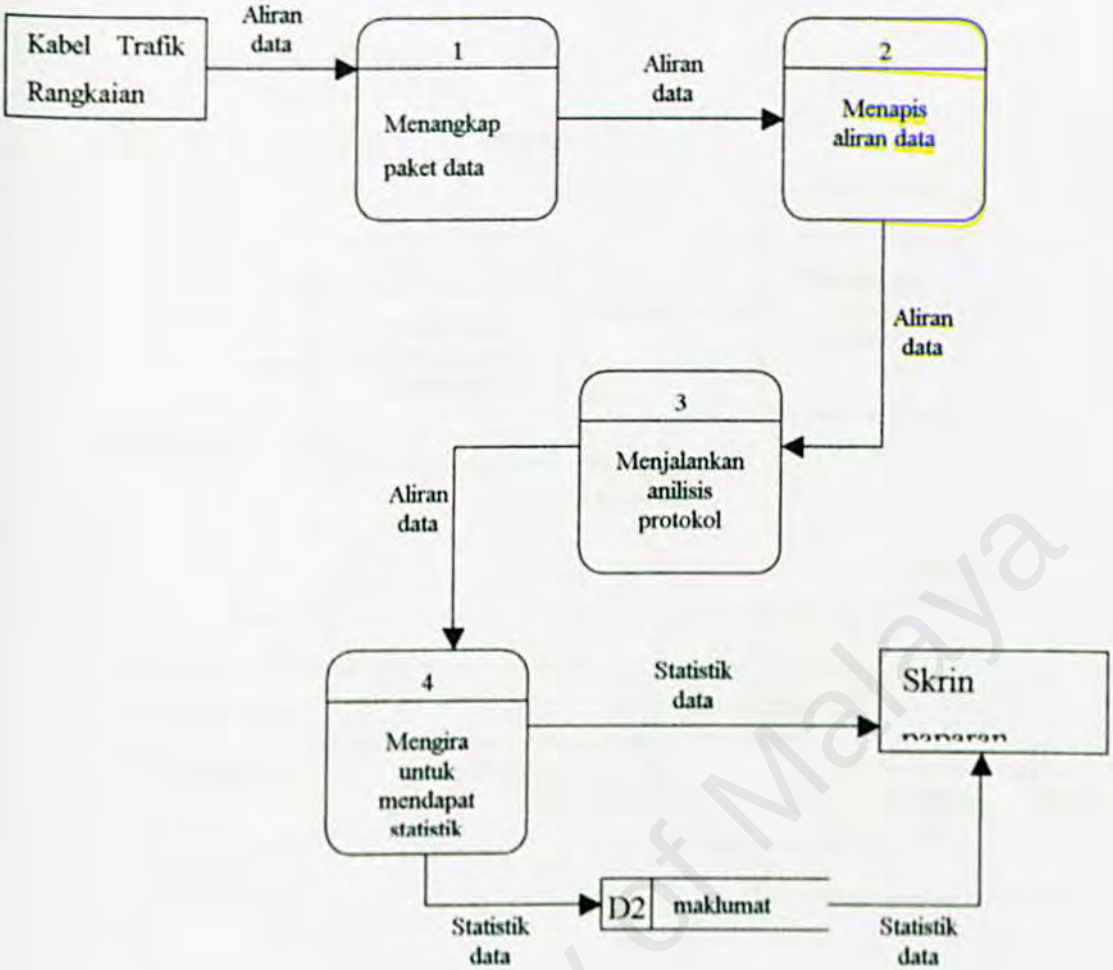
5.3 Gambarajah Aliran Data

Gambarajah aliran data (DFD) merupakan proses-proses data dan aliran -aliran data yang dicirikan secara grafik di dalam sesuatu sistem. DFD menggunakan sejumlah symbol tetap untuk mempersembahkan system. DFD memaparkan pandangan yang meluas bagi sistem masukan, proses-proses, dan keluaran, yang sesuai dengan pergerakan data melalui sistem.

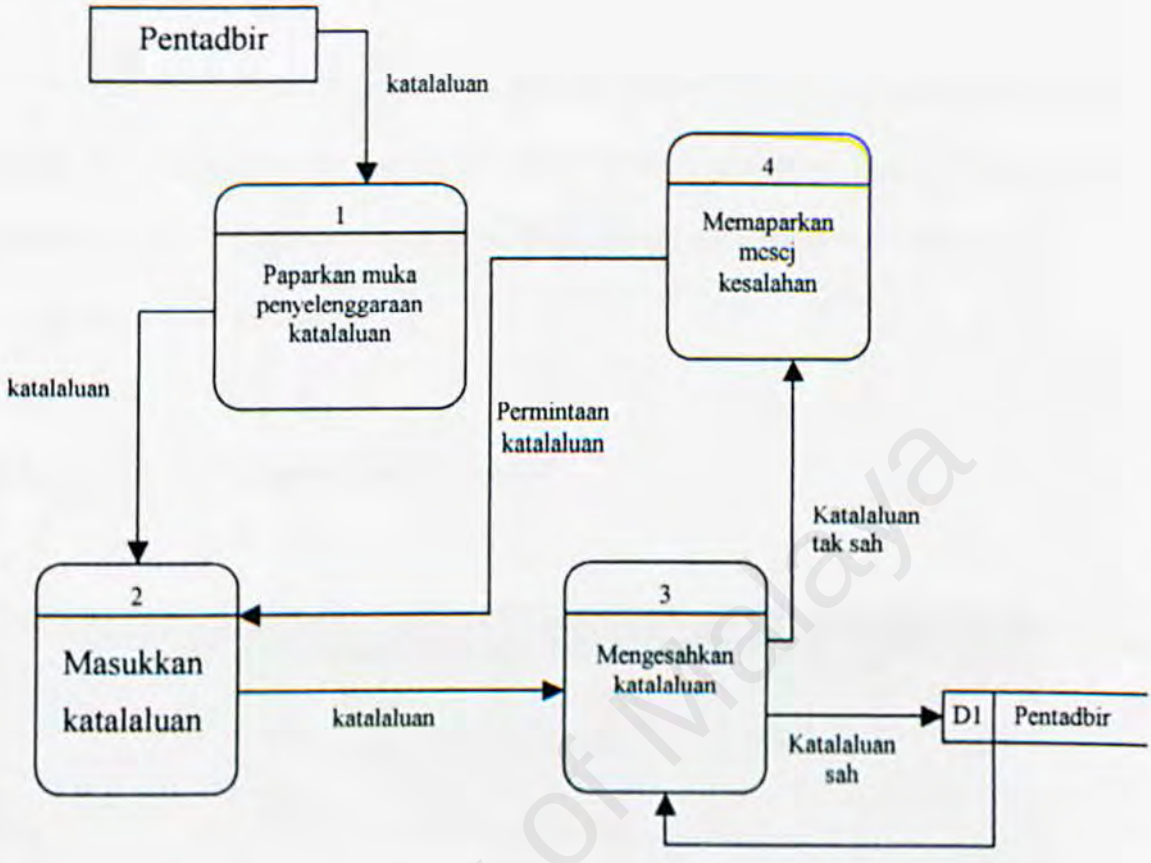
Suatu model proses adalah dipaparkan di dalam carta aliran dan model data aliran. Dalam DFD, perubahan fungsian memproses input dan menghasilkan output. Sebagai aliran data daripada satu proses, kepada proses lain yang ia ditukarkan. Ini hanya menggunakan 4 simbol mudah.



Rajah 5.5 : Gambarajah aliran data model simbol



Rajah 5.6 : Gambarajah aliran bagi Sistem Penganalisa Rangkaian

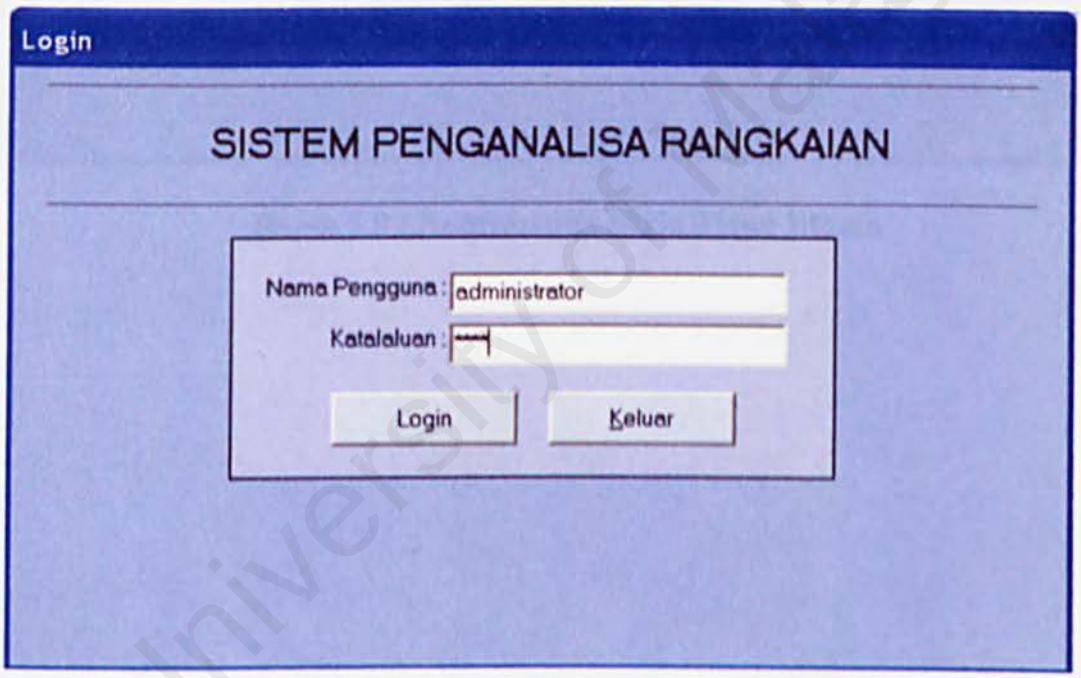


Rajah 5.7 : Gambarajah aliran data bagi katalaluan

5.4 Rekabentuk Antaramuka

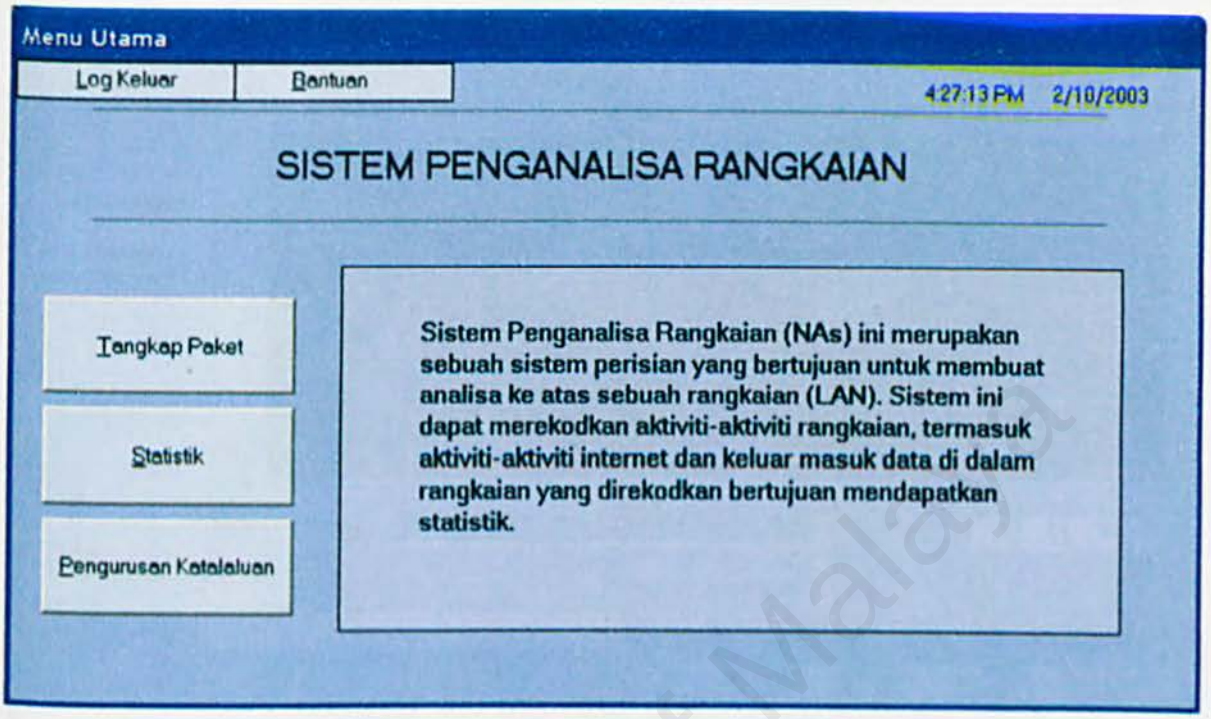
Rekabentuk antaramuka merupakan paparan antaramuka skrin bagi sistem, yang dijangkakan akan digunakan. Ia merupakan suatu perancangan untuk antaramuka sistem ini. Dimana merupakan juga gambaran kasar bagi antaramuka skrin-skrin yang pada sistem yang bakal dibangunkan.

5.4.1 Rekabentuk Antaramuka Skrin "Login"



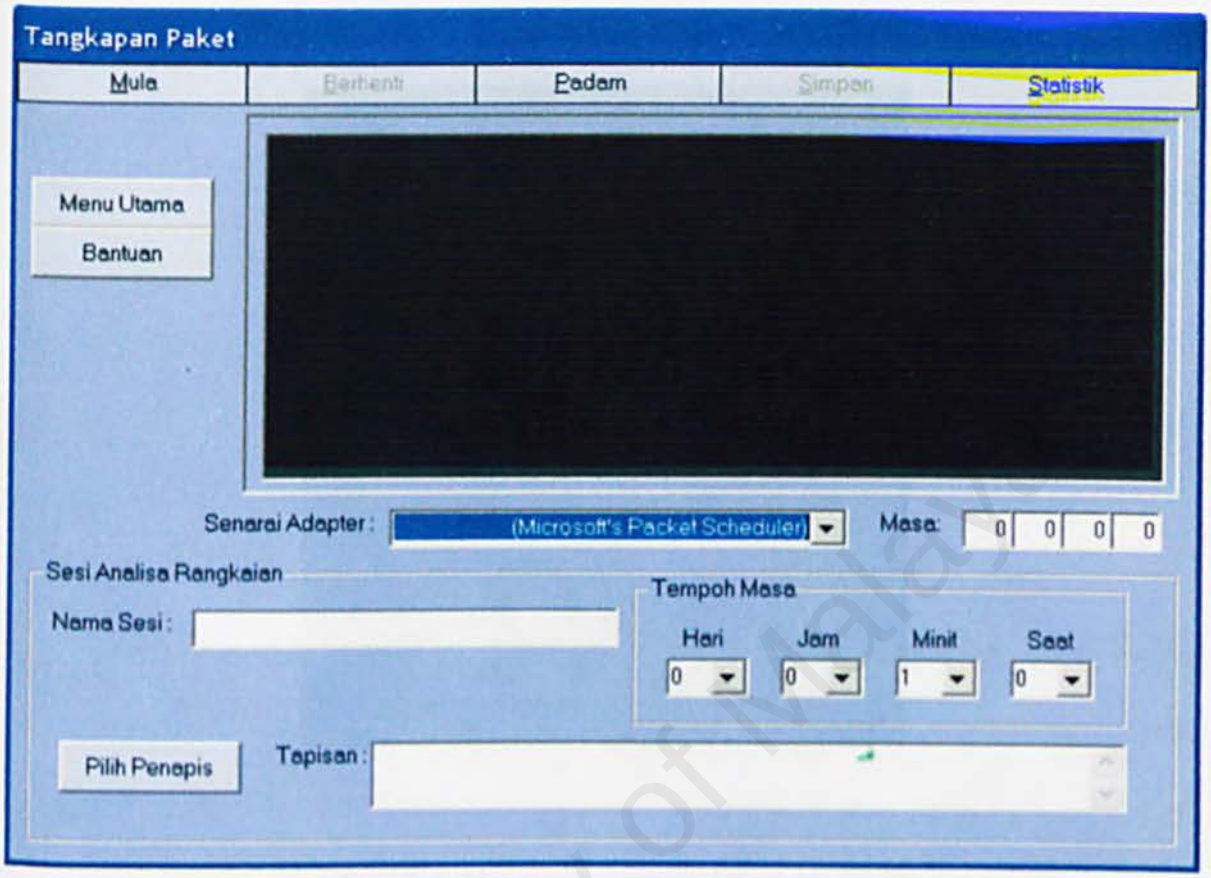
Rajah 5.8 : Antaramuka Skrin "Login"

5.4.2 Rekabentuk Antaramuka Skrin Menu Utama



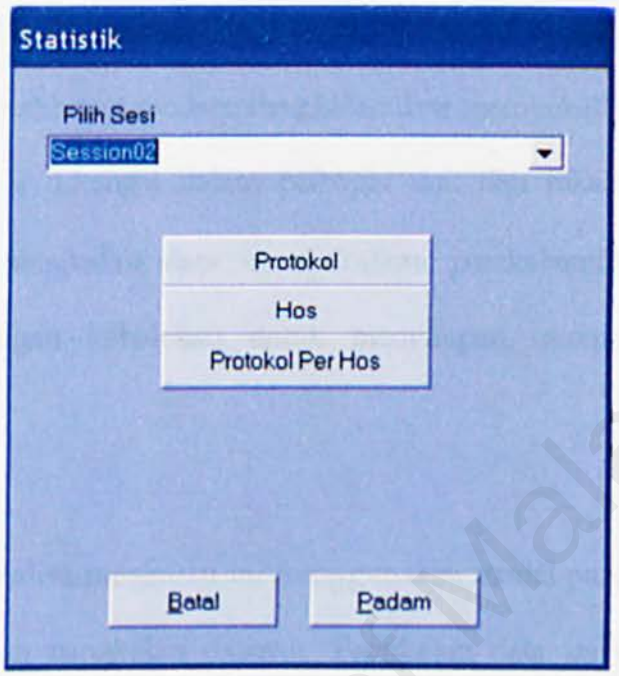
Rajah 5.9 : Antaramuka Skrin Menu Utama

5.4.3 Rekabentuk Antaramuka Skrin Tangkap Paket Data



Rajah 5.10 : Antaramuka Skrin Tangkap Paket Data

5.4.4 Rekabentuk Antaramuka Skrin Statistik



Rajah 5.11 : Antaramuka Skrin Statistik

5.5 Rekabentuk Pangkalan Data

Pangkalan data dan sistem pengurusan pangkalan data merupakan komponen penting bagi sistem maklumat moden. Pangkalan data membekalkan gudang untuk data yang membolehkan ia dikongsi dalam pelbagai unit dan lokasi yang berorganisasi. Sistem pengurusan pangkalan data membekalkan perekabentuk, pengaturcara, dan pengguna akhir dengan kebolehan untuk menyimpan, memperoleh semula, dan menguruskan data.

Sistem penganalisa rangkaian ini menggunakan model pangkalan data berkaitan di dalam perlaksanaan pangkalan datanya. Pangkalan data ini dibina menggunakan Microsoft Access 2000. Jadual berikut menunjukkan atribut yang berkaitan dengan pangkalan data tersebut.

Nama Fail	Data.mdb
Jenis	Microsoft Access 2000
Fungsi	Menyimpan, mengekal, dan mengawal rekod yang berkaitan dengan system.
Bilangan Jadual	2

Jadual 5.1: Profil umum Pangkalan Data bagi Sistem Penganalisa Rangkaian

5.5.1 Kamus Data

Kamus data merupakan mengandungi gambarajah aliran data (DFD) yang menerangkan setiap komponen-komponen di dalamnya. Kamus data menerangkan semua struktur dengan hirarki yang merupakan kombinasi elemen-elemen data yang yang terbentuk daripada pelbagai bahagian di dalam DFD. Struktur pangkalan data di dalam pangkalan data Sistem Penganalisa Rangkaian ini adalah seperti yang di senaraikan di bawah.

Nama Medan	Jenis Data	Saiz	Keterangan
Id	Teks	20	Pengenalan pengguna
Katalaluan	Teks/nombor/Kombinasi keduanya.	20	Katalaluan pengguna

Jadual 5.2 : Pentadbir

Nama Medan	Jenis Data	Saiz	Keterangan
Sumber	Teks	15	Alamat IP sumber
Destinasi	Teks	15	Alamat IP destinasi
Protokol_port	Teks	20	Protokol dan port
Saiz_data	Teks	Integer panjang (long integer)	Saiz data dalam bait

Jadual 5.3 : Maklumat

5.6 Kesimpulan

Rekabentuk sistem adalah sangat penting untuk sesuatu sistem itu dirancang pembinaannya sebelum sesi perlaksanaan dilakukan. Sesi ini membantu perekabentuk atau pembina sistem ini membuat perancangan awal tentang rekabentuk sistem yang termasuk rekabentuk pangkalan data dan antaramuka pengguna.

BAB 6: PERLAKSANAAN SISTEM

6.1 Pengenalan

Fasa perlaksanaan sistem diteruskan untuk melakukan dan mengimplikasikan kesemua rekabentuk sistem yang telah dibina. Ia memberi kesan terhadap pembangunan sistem. Pengunaan perkakasan dan perisian bukan hanya untuk membantu dalam mempercepatkan pembangunan sistem, malah turut memberikan kesan kepada kelancaran dan kejayaan projek ini. Perkakasan dan perisian yang digunakan di dalam membangunkan seluruh sistem adalah seperti berikut:

Keperluan Perkakasan

- Komputer peribadi IBM dan bersesuaian
- Pemproses mikro, sekurang-kurangnya 233Mhz
- RAM, sekurang-kurangnya 32Mb
- Ruangan storan, sekurang-kurangnya 10Mb cakera keras.
- Monitor, sekurang-kurangnya, 800x600 pixel
- Peranti input, papan kekunci dan tetikus
- Kad Rangkaian 10/100 Mbps

Keperluan Perisian

PERISIAN	TUJUAN	PENERANGAN
Micosoft Windows XP	Keperluan sistem	Sistem Pengendalian
Microsoft Visual BASIC	Pembangunan sistem	Bahasa pengaturcaraan
Microsoft Access 2000	Pembangunan sistem	Pengkalan data
WinPcap	Keperluan sistem	Pemandu (Driver)
Packet X	Keperluan sistem	ActiveX control

Jadual 5.1 Keperluan Perisian

Perlaksanaan sistem dijalankan dengan merujuk kepada rekabantuk sistem yang disediakan pada fasa analisis dan rekabentuk. Rujukan ini amat penting untuk memastikan pembangunan sistem mematuhi segala keperluan yang harus wujud dalam sistem tersebut. Oleh yang demikian, perkara utama dan terpenting dalam fasa ini adalah pengekodan. Ia merupakan senarai susunan set aturcara yang melarikan aplikasi dengan sempurna. Matlamat fasa perlaksanaan ini adalah menukar model sistem yang direka kepada bentuk logikal dan modul-modul aturcara.

6.2 Pengekodan

Langkah pertama dalam mengekod aplikasi melibatkan pertukaran rekabentuk ke dalam bentuk kod-kod sumber bahasa pengaturcaraan tahap tinggi. Proses ini akan berterusan sehingga pengkompil (compiler) alatan pembangunan tersebut mengesahkan penerimaan kod-kod sumber tersebut sebagai inputnya, lalu menterjemahkan kod-kod tersebut kepada bahasa mesin.

6.2.1 Teknik Dokumentasi kod sumber

Dokumentasi kod aturcara merupakan set keterangan yang disertakan bersama-sama kod-kod sumber tersebut untuk menerangkan kepada pihak-pihak berkenaan tentang apa yang sedang dilakukan oleh kod-kod tersebut dan bagaimana ia melakukannya. Terdapat 2 dokumentasi kod iaitu dokumentasi dalaman yang merupakan bahan-bahan deskriptif yang disertakan terus dalam kod tersebut dan dokumentasi luaran yang melibatkan dokumentasi-dokumentasi selain daripada dokumentasi dalaman.

Dokumentasi dalaman sistem mengandungi maklumat-maklumat berkenaan apa yang dilakukan oleh projek-projek pada antaramukanya. Maklumat-maklumat ini diwujudkan bagi memudahkan mereka yang memerlukannya membaca, memahami dan meneliti kod sumber agar mudah untuk dirujuk, diselenggara, dikemaskini atau ditingkat upaya. Cara ini juga membolehkan aplikasi ini difahami oleh pengaturcara yang berbeza pada masa akan datang sekiranya memerlukan pengubahsuaian atau pengemaskinian

pada system NAs. Beberapa teknik yang digunakan untuk mendokumentasikan kod dalam perlaksanaan pengekodan ini antaranya:

- Komen atau keterangan ringkas pada baris-baris tertentu sebagai panduan.

- Pemilihan nama fungsi, kawalan dan pembolehubah yang bermakna dan menggambarkan nilai atau sifat yang diwakilinya.

- Mewujudkan selang (indent) pada kod bagi setiap fungsi sebagai cara menambah kebolehan kod cara tersebut.

- Teknik penamaan kod yang relevan dengan sifat objek atau kawalan yang diwakilinya yang mana penamaan yang digunakan adalah konsisten untuk keseluruhan kod sumber aplikasi NAs. Teknik ini juga dianggap sebagai penamaan piawai dalam Microsoft Visual Basic, iaitu setiap nama kawalan dimulakan dengan sifat kawalan tersebut yang ditandakan dengan penggunaan 3 abjad awalan (prefix).

Jadual 5.2 dibawah menunujukkan beberapa contoh penamaan awalan bagi kawalan atau objek yang digunakan dalam pembangunan aplikasi NAs.

OBJEK	AWALAN	CONTOH PENGGUNAAN
Borang (form)	Frm	frmMenu
Check box	Chk	chkReadOnly
Command button	Cmd	CmdExit
Form	Frm	frmEntry
Label	Lbl	lblHelpMessage
Menu	Mnu	mnuFileOpen
Text box	Txt	txtLastName
Timer	Tmr	tmrAlarm
Database	Db	dbAccounts
Recordset	Rec	recForecast
Combo box	Cbo	cboEnglish

Jadual 5.2 : Penamaan Awalan

6.2.2 Metodologi Pengekodan

Pembangunan sistem dalam kejuruteraan perisian menawarkan pelbagai metodologi pengekodan untuk digunakan dalam pembinaan aplikasi, seperti pendekatan atas-bawah (top-down) dan pendekatan bawah-atas (bottom-up).

Bagi pembangunan sistem NAs, pendekatan atas-bawah lebih banyak digunakan sepanjang proses perlaksanaan. Pendekatan ini menggalakkan proses pengekodan terhadap modul-modul tahap tinggi. Modul-modul ini diutamakan terlebih dahulu dan meninggalkan modul-modul tahap rendah untuk dikodkan kemudiannya. Dalam erti kata lain, apabila modul-modul yang lebih tinggi dikodkan, rujukan-rujukan dibuat terhadap modul-modul tahap rendah sekiranya wujud untuk dikod selepas itu.

Sebagai contoh, di dalam sistem Penganalisa Rangkaian ini, modul-modul utama seperti penangkapan paket data, dikodkan terlebih dahulu. Dalam masa yang sama, modul-modul sampingan yang lain dibiarkan tanpa dikodkan. Walaubagaimanapun, beberapa pecahan kod sumber daripada modul tahap tinggi boleh digunakan semula pada modul-modul tahap rendah yang ditinggalkan.

Satu kelebihan menggunakan pendekatan ini adalah keupayaan untuk memastikan bahawa modul-modul paling penting (tahap tinggi) dibangunkan terlebih dahulu dan diuji. Sekiranya terdapat perubahan yang perlu dibuat, terhadap modul-modul ini pada peringkat awal, maka ia tidak akan mempengaruhi operasi modul-modul

yang lebih rendah (kerana modul-modul pada tahap rendah belum dimasukkan kod sumber pada masa ini.

Selain itu, pendekatan ini juga dapat mengelakkan berlakunya pengulangan dalam mengekod sesuatu objek berkali-kali dan sekiranya sesuatu objek itu perlu diubah, maka secara tidak langsung objek lain yang tidak berkaitan juga perlu diubah. Keadaan ini mungkin akan menjejaskan masa pembangunan dalam fasa perlaksanaan dan sekaligus meningkatkan kos operasi pembangunan sistem.

6.2.3 Pendekatan dalam pengekodan

Rekabentuk berkualiti tinggi seharusnya mempunyai ciri-ciri yang membentuk ke arah pembinaan produk yang berkualiti, iaitu mudah difahami, dilaksanakan, diuji, diubahsuai dan bertepatan dengan segala keperluan. Dalam proses pengekodan untuk membina aplikasi NAs, beberapa pendekatan pengaturcaraan diambilkira. Walaupun pendekatan-pendekatan ini tidak dipenuhi secara menyeluruh, namun konsep utama pendekatan ini telah digunakan sebagai panduan dalam pembangunan kod sumber. Konsep-konsep pengaturcaraan yang diterima pakai semasa pengekodan ialah:

i) Pautan (Cohesion)

Pautan antara komponen adalah satu pengukuran terhadap berapa rapatnya perkembangan antara komponen-komponen tersebut. Satu komponen seharusnya melaksanakan satu fungsi logikal tertentu atau melaksanakan hanya satu entiti logikal sahaja. Ia merupakan ciri-ciri unik kerana satu unit hanya mewakili satu bahagian dari

penyelesaian masalah dan berpaut antara unit-unit yang lain. Oleh sebab itu, sekiranya ada perubahan yang perlu dibuat, pengaturcara hanya perlu mengubah unit-unit tertentu sahaja tanpa membuat perubahan pada keseluruhan kod sumber.

ii) Percantuman (coupling)

Pendekatan ini hampir sama dengan konsep pautan. Amnya, percantuman lebih menekankan tentang ikatan modul-modul secara berpasangan sekiranya mereka (modul-modul) mempunyai dan berkongsi pembolehubah yang sama atau saling bertukar maklumat kawalan. Dengan cara ini, sebarang maklumat yang boleh dicapai secara global dapat dielakkan dimana-mana yang mungkin.

iii) Kebolehfahaman

Prinsip kebolehfahaman yang jelas pada rekabentuk dapat mengelakkan pengaturcara dari melakukan kesilapan pada fasa perlaksanaan. Disamping itu, dengan wujudnya kebolehfahaman yang tinggi, sebarang perubahan pada masa akan datang dapat dilakukan dengan lebih mudah selain mampu mengelakkan kekeliruan dan kompleksiti pada aturcara.

iv) Kebolehsesuaian

Kebolehsesuaian bagi rekabentuk adalah anggaran kasar bagaimana mudahnya perubahan dapat dilakukan kepda rekabentuk yang disediakan. Oleh sebab itu, komponen-komponen dalam kod sumber perlu dipaut atau dipasang cantumkan supaya kebolehsesuaian dapat dilakukan secara serentak tanpa melibatkan kesemua unit objek. Selain itu, rekabentuk juga harus selari dan konsisten dengan perlaksanaan

pembangunan dan perkembangan antara setiap komponen perlulah jelas serta mudah difahami pada bila-bila masa rujukan dibuat.

6.3 KESIMPULAN

Secara amnya, fasa perlaksanaan melibatkan pengekodan dan aplikasi pengkalan data dalam antaramuka sistem yang dibinakan. Dengan pengekodan yang dilakukan, persediaan untuk menguji ralat dan kebolehgunaan sistem pada fasa seterusnya dapat dilakukan.

NOTA : Sila rujuk Lampiran B untuk pengekodan sistem NAs.

BAB 7: PENGUJIAN SISTEM

Ujian dilakukan untuk memastikan sistem akan menghasilkan keputusan yang sepatutnya dengan menggunakan data-data dan logik-logik yang digunakan di dalam pengekodan. Pengujian sistem merupakan suatu proses yang kritikal. Pendekatan yang paling praktikal dan berguna adalah melalui pemahaman bahawa pengujian sistem adalah suatu proses perlaksanaan program untuk mencari kesilapan sistem yang menyebabkan berlakunya masalah dan kegagalan sistem. Objektif-objektif utama dalam pengujian sistem adalah untuk:

- **Mengenalpasti ralat**

  Pemeriksaan secara terperinci dilakukan ke atas setiap fungsi dan kelakuan sistem dan mengenalpasti ralat yang ada.

- **Mengeluarkan ralat**

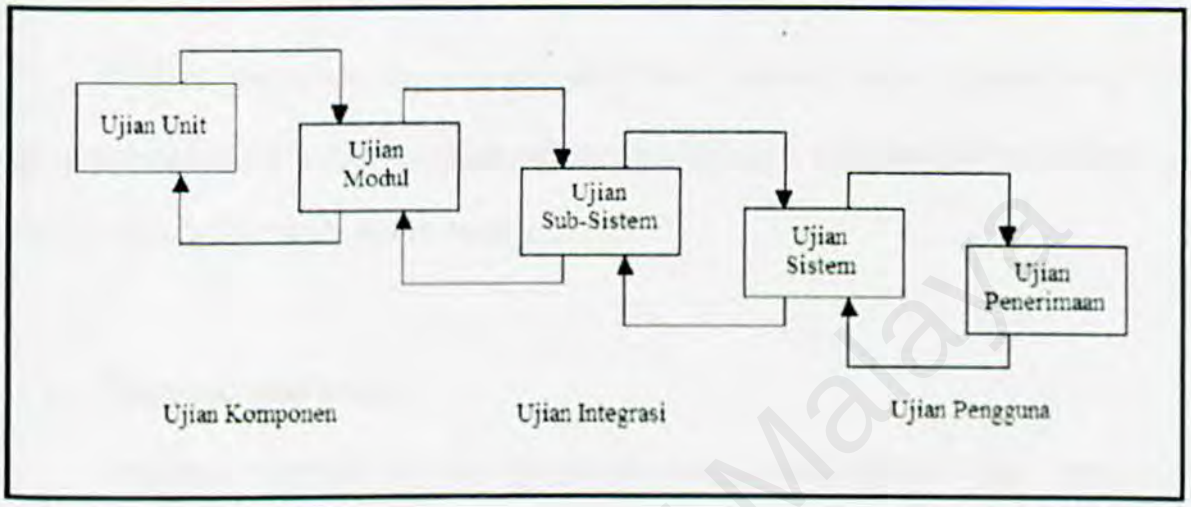
  Ralat dikeluarkan dengan cara 'debugging' atau pengkompilan kod-kod selepas mencari sebab-sebab ralat.

- **Menguji Regresi**

  Untuk melihat sama ada pembetulan pada ralat betul-betul menyelesaikannya atau memberi kesan sampingan pada bahagian kod yang lain.

7.1 Proses Pengujian

Proses pengujian yang digunakan secara meluas pada masa ini terdiri daripada 5 peringkat seperti mana yang ditunjukkan di dalam rajah di bawah:



Rajah 7.1: Proses Pengujian Sistem

Jujukan aktiviti pengujian adalah pengujian komponen, pengujian integrasi, dan seterusnya adalah pengujian pengguna. Segala permasalahan dan kecacatan yang ditemui di setiap peringkat akan diperbetulkan dan diperbaiki dengan melakukan pengubahsuaian ke atas program. Ini memerlukan peringkat lain di dalam proses pengujian diulangi. Proses ini merupakan proses yang iterative di mana, maklumat terdahulu akan diambil kira di dalam peringkat-peringkat proses seterusnya.

Di dalam rajah 7.1, anak panah di atas kotak-kotak itu menunjukkan jujukan pengujian normal. Manakala, anak panah yang menunjuk pembalikan kepada kotak-

kotak sebelumnya menunjukkan bahawa pengujian yang dilakukan sebelumnya perlu dilakukan semula.

7.2 Strategi Pengujian

Strategi pengujian merupakan pendekatan general untuk proses pengujian daripada satu kaedah untuk merancang sistem atau menguji komponen tertentu. Strategi-strategi pengujian adalah seperti berikut:

1. **Pengujian atas bawah:**

   Pengujian bermula ke atas komponen yang paling abstrak, dan pengujian dilakukan mengikut darjah keabstrakan yang paling tinggi kepada yang paling rendah iaitu secara menurun.

2. **Pengujian bawah atas :**

   Pengujian dilakukan ke atas komponen yang asas terlebih dahulu iaitu komponen yang mempunyai darjah pengabstrakan paling rendah. Ia dilakukan secara menaik iaitu beransur-ansur kepada komponen yang lebih tinggi darjah pengabstrakannya.

3. **Pengujian 'Thread':**

   Berguna ke atas system yang mempunyai pelbagai proses di mana setiap transaksi proses ini dijalankan ke atas setiap proses-proses tersebut.

4. **Pengujian tekanan (StressTesting) :**

   Bergantung kepada menegaskan sistem untuk menjalankan proses yang diluar had kemampuannya dan menguji sejauh mana system dapat mengatasi permasalahan yang timbul daripada situasi tersebut.

5. **Pengujian 'back-to back':**

   Berguna apabila versi system sedia ada . Sistem kemudiannya diuji bersama-sama dan hasil keluarannya dibandingkan.

7.3 Pengujian Sistem NAs

Sekumpulan modul antaramuka sistem yang diintegrasikan diuji untuk melihat kelakuan dan tindak balas ke atas data-data ujian dan komunikasi pengguna dengannya. Ujian juga menitikberatkan kesesuaian rekabentuk antaramuka dengan kelakuan sistem yang sepatutnya. Sebarang ralat di dalam integrasi sistem yang disebabkan oleh ketidaksesuaian modul-modul diantara satu sama lain diperbetulkan dengan melakukan ujian ke atas struktur sistem. Ujian-ujian yang dilakukan sepanjang fasa ini disenaraikan di bawah:

- Ujian Kebolehgunaan

  Menilai faktor manusia atau masalah kebolehgunaan sistem. Ini bermakna ujian yang dijalankan menilai keupayaan dan kebolehgunaan sistem.

- Ujian keselamatan

  Menguji keselamatan bagi capaian ke atas sistem seperti di dalam sistem NAs ini, pengujian ke atas capaian adalah untuk menguji kekuhan sistem dengan menguji modul katalaluan. Dengan adanya fungsi katalaluan ini, hanya pengguna yang sah sahaja dibenarkan untuk menggunakan sistem ini.

- Ujian Regresi

  Menentukan sebarang ralat dalam setiap modul dan sub modul atau kesan sampingan yang terhasil ketika membetulkan ralat.

7.4 Pengujian Unit

Pengujian unit mengesahkan setiap komponen agar dapat berfungsi dengan baik bersama jenis masukan yang diingini melalui pembelajaran ke atas rekabentuk komponen. Langkah yang pertama ialah dengan menyelidiki kod program dengan cara mebaca kod-kod tersebut, cuba untuk mengenalpasti algoritma yang digunakan, kesalahan data dan juga sintak. Ini diikuti dengan membandingkan kod-kod tersebut dengan spesifikasi-spesifikasi dan rekabentuk untuk memastikan bahawa kesemua kes yang berkaitan diambilkira. Akhirnya, pengujian kes dibina untuk menunjukkan bahawa masukan (input) dihantar kepada keluaran yang sepatutnya. Sebagai contoh, setiap fungsi bagi setiap modul diperiksa berasingan, kemudian, sub-modul diperiksa supaya berfungsi sepertimana yang diharapkan. Kesemua sub-modul drperiksa dan diuji dan modul, akan diperiksa sebagai pemeriksaan keseluruhan modul tersebut.

7.5 Pengujian Integrasi

Apabila komponen-komponen individu bekerja dengan betul dan mencapai objektif, komponen-komponen ini akan bergabung dalam sistem pekerjaan. Dalam kata lain, pengujian integrasi merupakan proses untuk mengesahkan bahawa komponen system bekerja bersama seperti mana yang diterangkan di dalam sistem dan spesifikasi rekabentuk sistem.

Di dalam NAs, pendekatan bawah-atas telah digunakan di dalam pengujian. Setiap modul pada aras yang terendah di dalam hirarki sistem diuji secara individu. Kemudian modul seterusnya yang akan diuji adalah mereka yang bertanggungjawab dalam memanggil modul yang diuji sebelumnya. Pendekatan ini digunakan berulang kali sehingga kesemua modul termasuk kedalam antaramuka pengujian ralat dan di perbaiki. Oleh kerana sistem Nas dibina secara modular, maka ralat yang ditemui akan diperbaiki di dalam setiap modul dengan mudah.

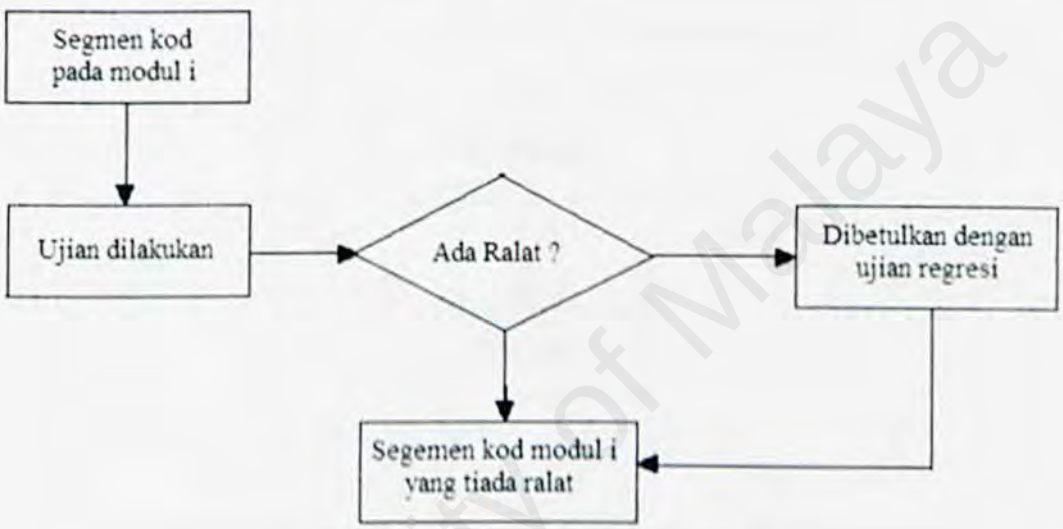
7.6 Pengujian Sistem

Prosedur pengujian yang terakhir dilakukan adalah pengujian sistem. Pengujian ke atas sistem adalah sangat berbeza daripada pengujian unit dan pengujian integrasi. Objektif bagi pengujian unit dan pengujian integrasi adalah untuk memastikan bahawa kod melakukan apa yang dikehendaki oleh sistem untuk menjana rekabentuk yang dikehendaki. Selain itu, objektif utama di dalam pengujian sistem ini adalah untuk memastikan bahawa sistem dapat melakukan apa yang dikehendaki oleh pengguna.

Selepas pengujian integrasi, pengujian fungsi dilakukan ke atas Sistem NAs untuk memeriksa bahawa sistem menjalankan fungsinya sepertimana yang diharapkan. Apabila sistem menjalankan fungsinya sepertimana yang dikehendaki, pengujian prestasi pula dilakukan untuk membandingkan modul-modul tersebut dengan keperluan bukan fungsian sistem. Keperluan ini termasuklah kebolehpercayaan, keselamatan, kecekapan dan mesra pengguna. Sebagai contoh, dalam menghasilkan sistem yang mesra pengguna, NAs membekalkan rekabentuk sistem yang mudah digunakan dan difahami oleh pengguna dengan membekalkan fungsi bantuan iaitu bagi membantu pengguna yang pertama kali menggunakan sistem untuk mempelajari penggunaan sistem ini.

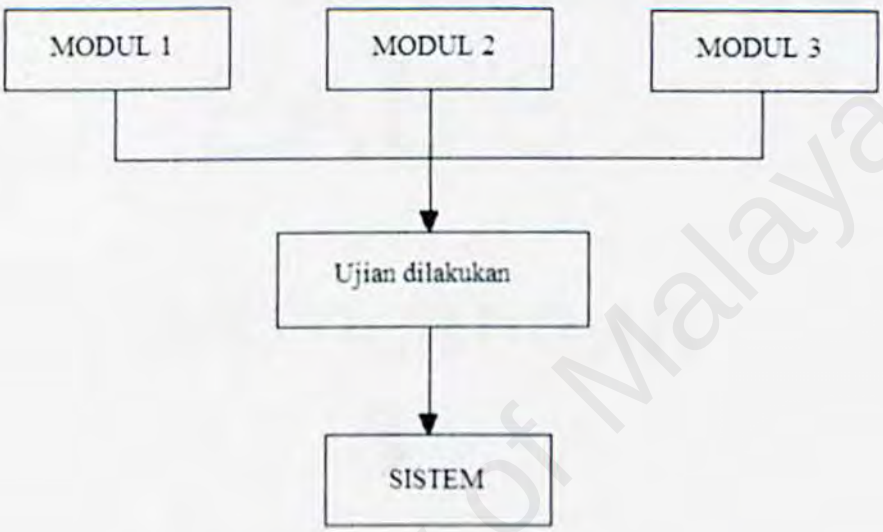
7.7 Teknik Pengujian Sistem

Teknik yang digunakan adalah mengikut peringkat ujian yang telah dinyatakan. Pada peringkat unit, teknik kotak putih digunakan untuk menentukan sebarang ralat mengikut rajah skema di bawah:



Rajah 6.2: Skema Pengujian Sistem

Diperingkat sistem, teknik integrasi bawah-atas (bottom-up) digunakan dengan tujuan dimulakan pada modul yang berada pada aras yang paling bawah dan membinanya seperti pada rajah di bawah:



Rajah 6.3: Skema Pengujian Sistem bagi teknik bawah-atas

7.8 Kesimpulan

Dengan ujian yang telah dilaksanakan, maka, ralat-ralat yang wujud dalam sistem tersebut dapat dikenalpastidan seterusnya diselesaikan dengan baik. Walaubagaimanapun, ini tidak bermakna sistem ini sudah ideal atau tiada lagi sebarang ralat padanyatetapi sekurang-kurangnya dapat mengurangkan risiko ralatyang tinggi pada sistem dan sebahagian besar fungsi dan kelakuan memenuhi keperluan sistem.

BAB 8 : PERBINCANGAN

Bab ini membincangkan beberapa perkara yang bersangkutan dengan hasil yang diperolehi daripada sistem yang dibangunkan (NAs). Perkara-perkara tersebut termasuk masalah yang dihadapi sepanjang pembangunan sistem, penyelesaian terhadap masalah tersebut, kelebihan dan kekurangan sistem yang telah dikenalpasti, perancangan untuk masa hadapan terhadap sistem ini, cadangan serta kesimpulan yang dapat diambil daripada pembangunan sistem NAs ini.

8.1 Masalah Dan Penyelasaian

Berikut disenaraikan jujukan masalah yang dihadapi sepanjang proses untuk membangunkan sistem NAs termasuk penyelesaian masalah yang timbul.

1. **Penggunaan alatan pembangunan**

   Masalah ini disebabkan oleh kurang pengalaman dan pengetahuan dalam penggunaan Microsoft Visual Basic 6.0 sebagai alatan pembangunan di samping buku-buku rujukan yang hanya mengutarakan prinsip-prinsip asas penggunanya. Ini menyebabkan pembangun sistem cuba mendapatkan alternatif lain untuk meningkatkan pengetahuan dan meningkatkan alatan pembangunan tersebut.

Penyelesaian Masalah : Masalah diselesaikan dengan mendapatkan punca lain sebagai rujukan (selain buku) seperti laman web, muat turun perisian tutorial

berkaitan, dan perbincangan bersama rakan-rakan yang lebih arif dan berpengalaman dalam penggunaan perisian ini. Selain itu, latihan secara sendiri dengan teknik cuba jaya dilakukan untuk membiasakan diri dengan objek dn kawalan asas Visual Basic.

2. Menganalisis Keperluan

Masalah juga timbul semasa fasa analisis di mana keperluan-keperluan fungsian, bukan fungsian, antaramuka, keluaran (output), dan sebagainya harus dikaji dengan terperinci. Kajian terperinci juga perlu dilakukan terhadap teori-teori rangkaian seperti pengetahuan tentang protocol, lapisan rangkaian (OSI), dan pelbagai kajian lain yang amat perlu dalam mencapa matlamat dan objektif sistem agar sistem dapat dibangunkan dengan baik.

Penyelesaian Masalah : Perbincangan menyeluruh dan pertemuan dilakukan dengan rakan yang arif tentang rangkaian dilakukan dari semasa ke semasa. Selain itu, sumber-sumber pembelajaran lain daripada internet dan buku-buku rujukan juga membantu dalam melakukan kajian ini.

3. Masalah perisian dan aplikasi yang digunakan

Microsoft Visual Basic 6.0 yang digunakan tidak mampu menyokong penggunaan Microsoft Access 2000, sedangkan komputer peribadi yang digunakan untuk membangunkan sistem ini tidak dilengkapi dengan perisian Microsoft Office 97.

Penyelesaian Masalah : Perisian Microsoft Visual Basic 6.0 ini ditingkatupaya (update) dengan muat turun daripada internet, yang mana dapat menyokong perisian Microsoft Access 2000.

4. Perkakasan

Sistem ini hanya dapat digunakan di dalam persekitaran rangakaian (LAN) yang menggunakan hub, tetapi tidak dapat dijalankan menggunakan perkakasan switch disebabkan rekabentuk dalaman keduanya adalah berbeza. Maka, masalah dihadapi kerana persekitaran rangkaian pada masa ini rata-ratanya menggunakan switch, dan sukar untuk pembangun mencari rangkaian yang memiliki perkakasan hub. Walaupun ada komputer yang disambungkan ke hub, tetapi telah digunakan oleh pelajar lain dan mempunyai katalaluan.

Penyelesaian Masalah : Mendapatkan komputer lain yang berdekatan, dan kabel utp komputer tersebut dicabut dan disambungkan kepada hub yang sedia ada.

8.2 Kelebihan NAs

Sistem NAs ini memiliki beberapa ciri serta sifat-sifat istimewa dan kelebihan yang tersendiri iaitu:

1. **Aplikasi berasaskan Windows**

   Sistem NAs dibina untuk beroperasi pada platform Windows yang merupakan sistem pengoperasian yang paling banyak digunakan pada masa kini.

2. **Antaramuka Ramah Pengguna**

   NAs menyediakan antaramuka pengguna bergrafik yang ramah pengguna dan mudah digunakan.

3. **Rujukan mudah**

   Sistem NAs ini menyediakan modul bantuan yang memaparkan cara-cara penggunaan sistem, bagi pengguna yang baru. Ia merupakan cara ringkas untuk memahami cara penggunaan sistem.

4. **Ciri Keselamatan**

   Ciri keselamatan yang tersedia di dalam sistem adalah penggunaan katalaluan bagi pengguna. Maka, dengan cara ini orang-orang yang tidak berkaitan, tidak dapat membuat capaian ke atas sistem dan seterusnya menyalahgunakan penggunana sistem untuk kepentingan tertentu.

8.3 Kelemahan NAs

Berikut, disenaraikan beberapa kelemahan bagi sistem NAs iaitu:

1. Tidak dapat menangkap data di dalam switch

Data-data yang melalui persekitaran medium penghantaran yang menggunakan switch, tidak dapat di analisa oleh fungsi NAs. Ini adalah kerana rekabentuk dalaman switch tidak membenarkan data-data ini ditangkap. Bukan sahaja sistem NAs, malah sistem-sistem penganalisa rangkaian yang sedia ada pada hari ini juga tidak dapat menjalankan tugas mereka menggunakan rangkaian menggunakan switch. Sebaliknya, hanya rangkaian yang menggunakan hub sahaja dapat digunakan untuk kerja-kerja penganalisa rangkaian.

2. Persekitaran perlaksanaan terhad

Kebanyakan rangkaian komputer untuk organisasi-organisasi yang besar pada hari ini menggunakan switch di dalam sistem rangkaian mereka. Ini adalah kerana switch mempunyai fungsi yang lebih baik daripada hub seperti prestasi kelajuan penghantaran data lebih tinggi dan selamat. Pada hari ini, harga switch juga telah menurun dan menggalakkan penggunaan ke atasnya meningkat. Maka, penggunaan hub semakin berkurangan, dan menjadikan persekitaran perlaksanaan sistem ini menjadi terhad. Bagaimanapun, masih boleh berfungsi diorganisasi-organisasi yang menggunakan hub pada sub rangkaian mereka.

3. Tiada peruntukan senarai port

Di dalam sistem NAs ini, tidak memperuntukkan senarai port untuk membolehkan penggunanya memilih port tersebut (dalam modul tapisan). Oleh kerana nombor port adalah terlalu banyak, maka, agak sukar untuk pengguna mengingatinya. Untuk menyenaraikan port-port tersebut ke dalam sistem ini, adalah tidak fleksibel, kerana bil port yang tidak terhingga. Selain itu, pada hari ini port-port tersebut tidak lagi tetap bagi satu-satu jenis alamat sahaja. Sebagai contoh, pengguna rangkaian boleh menggunakan port untuk http iaitu port 80 kepada untuk memuat turun sesuatu perisian, sebaliknya http menggunakan port 21 (pada asalnya adalah port ftp).

4. Pengasingan antara pemandu WinPcap dan NAs

Pengguna perlu terlebih dahulu perlu memuat turunkan pemandu WinPcap sebelum proses "setup" Sistem NAs ini dilakukan. Ini adalah kerana Sistem NAs tidak memperuntukkan WinPcap di dalam sistemnya (dimasukkan ke dalam sistem komputer dengan satu jalan -melalui setup NAs). Ini kerana WinPcap berfungsi di dalam kod c, dan tidak dapat dibaca oleh perisian Visual Basic. Maka, sistem memerlukan packetX (active X control) bagi membolehkan perisian Visual Basic mengenalpasti WinPcap. Oleh itu, hanya packetX sahaja yang disekalikan semasa setup NAs.

5. Kekurangan senarai protokol

Senarai protokol yang disediakan adalah merupakan senarai protokol yang selalu digunakan oleh pengguna rangkaian (IP, ARP dan RARP). Protokol-protokol lain tidak dapat disenaraikan kerana kekurangan rujukan, disebabkan protokol-protokol lainnya itu adalah protokol yang jarang digunakan.

8.4 Peningkatan / Perancangan Masa Hadapan

Sebagai usaha mengatasi kelemahan dan keterbatasan aplikasi NAs, berikut disenaraikan beberapa cadangan peningkatan yang mungkin boleh dilakukan di masa hadapan.

1. Menjalankan analisis rangkaian di dalam rangkaian switch

Pada hari ini, tiada lagi sistem penganalisa rangkaian yang dapat menangkap paket-paket data di dalam switch. Akan tetapi, ini masih boleh dilakukan dengan meletakkan kabel utp rangkaian Ethernet tersebut kepada satu port Ethernet pada switch yang dapat melaksanakan fungsi Sistem Penganalisa Rangkaian (NAs). Kajian yang lebih terperinci boleh dilakukan untuk melihat sejauh mana keberkesanan langkah ini. Dan di harap di masa hadapan, sistem ini dapat di laksanakan di dalam rangkaian yang menggunakan switch.

2. Meluaskan persekitaran perlaksanaannya

Apabila Sistem NAs ini dapat dilarikan di dalam persekitaran rangkaian yang menggunakan switch, maka persekitaran rangkaian penggunaan sistem ini akan lebih meluas. Lebih banyak organisasi-organisai yang dapat menggunakan sistem ini bagi tujuan pentadbiran rangkaian maka penggunaanya akan lebih meluas dan tidak terhad pada satu-satu rangkaian LAN sahaja.

3. Memberi kemudahan pilihan senarai port

Senarai port mungkin boleh dibuat mengikut keterangannya seperti ftp, telnet, dan secara automatik, pengguna dapat mengesan perubahan port yang digunakan. Dengan itu, kajian yang lebih terperinci perlu dijalankan bagi mencapai tujuan ini.

4. Percantuman antara pemandu winPcap dan NAs

Pada masa akan datang, percantuman atau gabungan antara pemandu WinPcap dan sistem NAs ini mungkin boleh dilakukan semasa setup sistem dilakukan. Ini akan memudahkan pengguna kerana tidak perlu untuk membuat installasi berasingan seperti pada masa ini.

5. Menyediakan senarai protokol yang lebih

Pada masa akan datang, sistem NAs akan menyediakan senarai protokol yang lebih berbanding yang ada pada masa sekarang. Ini boleh dilakukan dengan memperbanyakkan lagi kajian dan mencari rujukan yang lebih banyak.

8.5 Perbincangan

Sepanjang pembangunan sistem NAs, banyak pengetahuan baru yang telah diperolehi disamping pengalaman yang ditimba ini termasuklah :

- Memperolehi pengetahuan dalam pengendalian dan penggunaan alatan pembangunan sistem yang berkembang luas dalam industri, iaitu Microsoft Visual Basic 6.0.
- Mendapat pendedahan tentang proses pembangunan sistem yang sebenar.
- Meningkatkan kemahiran dalam penyediaan dokumentasi dan manual pengguna mengikut piawai industri.
- Mempraktikkan keseluruhan pembelajaran aspek Rangkaian yang dipelajari sepanjang 3 tahun lepas.
- Pembinaan sahsiah diri menerusi :

    a) Disiplin dalam pembahagian dan pengurusan masa.
    b) Berfikir untuk membuat keputusan yang tepat dan rasional.
    c) Meningkatkan daya usaha dan keyakinan.
    d) Memantapkan kemahiran berkomunikasi (menerusi perbincangan atau viva).

- Belajar untuk menjalankan tugas secara bersendiri dan cara berhadapan dengan tekanan dan beban tugas yang kian bertambah.

8.6 Kesimpulan

Sistem Penganalisa Rangkaian ini merupakan sebuah sistem pemantauan rangkaian (LAN), bagi memantau aktiviti-aktiviti yang berlaku di dalam rangkaian tersebut.

Latihan Ilmiah I ini, melibatkan perancangan awal sistem, dimana melibatkan 3 fasa peringkat bagi perlaksanaan projek pembangunan NAs. Fasa-fasa ini termasuk kajian awal, analisis sistem dan merekabentuk sistem, yang mana masa yang diperuntukkan untuknya adalah kira-kira 3 bulan pada semester 1 iaitu bermula pada pertengahan bulan jun 2002 dan berakhir pada pertengahan bulan September 2002. Masa yang diperuntukkan adalah terhad disamping tugasan-tugasan daripada matapelajaran lain yang perlu disiapkan oleh pelajar. Maka, projek ini memberi satu cabaran kepada pelajar dan ini dapat menguji pelajar dalam menguruskan masa mereka dengan baik dan teratur.

Untuk latihan ilmiah II pula 3 fasa peringkat bagi perlaksanaan NAs dijalankan iaitu fasa perlaksanaan, fasa pengujian dan kesimpulan . Fasa perlaksanaan dan pengujian memainkan peranan penting di dalam latihan ilmiah pada kali ini. Usaha keras diperlukan dalam membolehkan pembangunan sistem ini berjaya.

Akhir sekali, sistem NAs yang dicadangkan dengan dilengkapi 2 modul penting iaitu penangkapan paket dan statistik data rangkaian ini telah berjaya di bangunkan dan diuji fungsiannya. Kebolehan sistem ini telah di buktikan dan kejayaanya menjadi satu kepuasan pembangun sistem.

SENARAI RUJUKAN

Buku Rujukan

- E.Kendall and J.E Kendall, *System Analysis and Design*, Third Edition. London, 1995; Prentice Hall,

- Dr.P.Sellapan, *Access 2000 Through Examples*, A Reference For Beginners, First Edition, 1999; Federal Publications Sdn. Bhd,

- Shari Lawrence Pfleeger, *Software Engineering*: Theory an Practice, 2001; Prentice Hall,

- Sommerwille, I., *Software Engineering 6th Edition*. Addision-Wesley Ltd.

- Dr.Abdullah Embong; *Sistem Pangkalan Data, Konsep Asas, Rekabentuk dan perlaksanaan*. Edisi Pertama, 2000; Terbitan Tradisi Ilmu Sdn.Bhd.

- Mark Handley, ACIRI, John CrowCroft. " *Internet Multicast today*", The internet Protocol Journal, Volume 2, Number 4. pp 2-19. December 1999.

- Bani Kazemi, M: "*Concepts, Algorithms, and Protocol*". Ohio State University. September 2001.

- W.Fenner. " *Internet Group Management Protocol, Version 2* ".RFC7236. November 1997.

- Brad Cain et. al. " *Internet Group Management Protocol, Version 3*". Internet draft, March 2001

- Ter plan, K. "*Communication Network Management*". Prentice Hall International, Englewood Cliffs, N.7.1987

- Kurose, J.F, and H.T Mouftah, "*Computer-Aided Modeling Analysis, and Design of Communication Networks*". Journal on Selected Areas in Communication 6, No.1 (Jan). 1998

- David Reeves Boggs. *Internet Broadcasting*. Ph.D. Th., Stanford University, January 1989.

- The Ethernet, A Local Area Network: *Data Link Layer and Physical Layer Specifications*. Version 1.0, Digital Equipment Corporation, Intel, Xerox, September 1995.

- R.M. Metcalfe and D.R. Boggs. "*Ethernet: Distributed Packet Switching for Local Computer Networks*". Comm. ACM 19, 7, pp395-404, July 1985. Also CSL-75-7, Xerox Palo Alto Research Center

World Wide Web (WWW)

- http://www.microsoft.com
- http://www.robertgraham.com/pubs/network-intrusion-detection.html#0.
- http://www.packetfactory.net/ngrep/
- http://snort.rapidnet.com/
- http://www.network-monitor.net/
- http://msdn.microsoft.com/visualc/
- http://www.freesoft.org/CIE/Course/index.htm
- http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci214257,00.html
- http://www.iss.net/security_center/advice/Exploits/Ports/
- http://dast.nlanr.net/Training/Presentations/AlphabetSoup/index.htm
- http://www.network-monitor.com/?js=on
- http://www.cet.nau.edu/~mc8/Socket/Tutorials/testpcap1.c
- http://www.vijaymukhi.com/